

# **IR PRO T1/E1 Leased Line Router**

---

# **User Manual**

**First Edition  
May 2000**

## **FCC Statement**

**Note:** This digital equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential installation. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used in accordance with the installation manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures :

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with part 15 of the FCC rules, Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

### **Warning:**

Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

## **CE Approved**

This digital device has been CE Approved.

## **Table of Contents**

<b>1 - Introduction 1-1 .....</b>	
IR PRO Application diagram.....	1-1
Package Contents .....	1-2
Pre-Installation Check List .....	1-2
Requirements	
Software Requirements.....	1-3
Hardware Requirements .....	1-3
Features and Benefits	
Features and Benefits .....	1-4
Some IR PRO FAQ.....	1-5
Net-Device Utilities	
Net-Device Setup Wizard .....	1-6
Net-Device Manager .....	1-6
Net-Device Monitor .....	1-6
 <b>2 - Setup Wizard 2-1</b>	
Select the Device you wish to Configure .....	2-2
Set the Device's IP address and name .....	2-3
Port function .....	2-4
IP Routing .....	2-6
Remote Access.....	2-7
DNS IP Address .....	2-9
Modem and baudrate settings. ....	2-10
Finish.....	2-11
Setup Wizard Completed.....	2-12
 <b>3 - Net-Device Manager 3-1</b>	
General Settings .....	3-2
LAN Ethernet Segment .....	3-2
Sync Port	
PPP Routing Settings .....	3-3
IP Routing .....	3-3
Authentication Method .....	3-5
Callback Settings .....	3-6
RADIUS Authentication .....	3-7
Frame Relay .....	3-8
Advanced Settings.....	3-9
Async Port	
IP Routing Settings.....	3-11
Allows Remote Dial-in .....	3-12
Authentication Method.....	3-12
Callback Settings .....	3-13
RADIUS Authentication .....	3-15
Remote Access .....	3-16
Enable IP Mapping.....	3-17
Port Settings (Asyn. Port),, .....	3-19
Edit Login Script.....	3-20
Login script examples.....	3-22
Modem String Settings .....	3-24
Dial-up / Hang-up Settings .....	3-25
ML-PPP.....	3-26
LAN DHCP Server .....	3-28
Routing Settings .....	3-30
Routing Table .....	3-31

Dynamic Routing .....	3-32
Filter Settings .....	3-34
Privileged Clients .....	3-38
Refresh Device List.....	3-39
Device Name and Password .....	3-40
Save Settings to File .....	3-41
Load Settings .....	3-42
Upgrade Firmware .....	4-43
General Diagnostic .....	4-44
 <b>4 - Net-Device Monitor 4-1</b>	
	4-2
Refresh Device List.....	4-2
Test connection .....	4-2
Terminate connection .....	4-2
Save to file	
Save Now .....	4-3
Autosave .....	4-3
IP address / name .....	4-4
Event message .....	4-4
TCP / IP tab .....	4-5
Connection time tab .....	4-6
Status tab .....	4-7
 <b>5 - Remote Access Settings .....</b>	<b>5-1</b>
 <b>6 - LAN-to-LAN Settings .....</b>	<b>6-1</b>
 <b>7 - Trouble Shooting.....</b>	<b>7-1</b>
 <b>8 - Tools for your EtherAccess.....</b>	<b>8-1</b>
 <b>9 - Glossary .....</b>	<b>9-1</b>

## INTRODUCTION

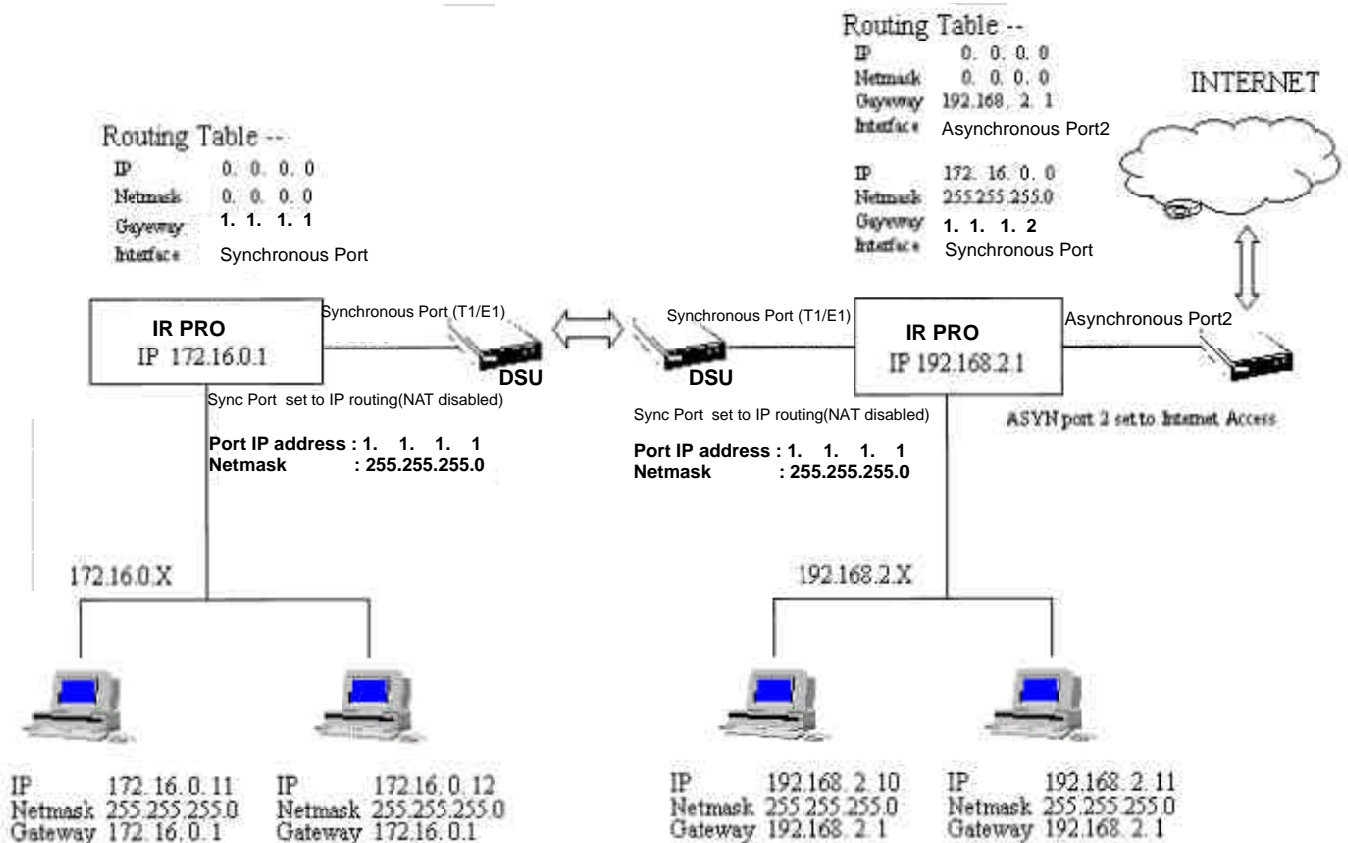
This manual will explain how to use the included Net-Device Utilities to configure and to monitor your IR PRO (Network Device).

The Network Device allows an entire LAN access to the remote office or Internet via the T1/E1 leased line or async port on any modem or ISDN TA. The router is equipped with: 1 sync port, 2 async port and a 10/100 Base-T uplink port (to extend to an external hub).

The asynchronous ports also allows remote users to dial-in to the device to access the network resources (Remote Access) or to dial-up to another router to connect to another branch's LAN (LAN-to-LAN).

### IR PRO provides your LAN with:

- A Internet Access Router
- A LAN-to-LAN Router
- A Remote Access Server



Application Diagram

## **PACKAGE CONTENTS**

Please inspect your package. The following items should be included:

- 1) The IR PRO unit
- 2) Power Adapter
- 3) One Net-Device Utilities CD
- 4) User manual (what you are reading)

If any of the above items are damaged or missing, please contact your dealer as soon as possible.

## **PRE-INSTALLATION CHECKLIST**

### **Before installing the IR PRO, you should**

- \* Carefully read the entire manual.
- \* Make sure you are familiar with the terminology and concepts of Windows. This guide works under the assumption that you know how to `get around` using Windows.
- \* Ensure that you meet all hardware and software requirements.

## **SOFTWARE REQUIREMENTS**

For Windows Installation

- Windows 95/98/2000, Windows NT 3.5 or higher
- Windows TCP/IP protocol installed
- Any Windows communication application for Dail-Out operation
- Any PPP supported communication application for Dail-in operation

## **HARDWARE REQUIREMENTS**

- 486 or higher purchase
- 10/100 Base-T cable to connect the IR PRO to the network
- One (or more) modem or ISDN TA
- One leased line DSU/CSU
- One standard serial cable to connect the modem to the IR PRO
- One V.35,V.25 serial cable to connect the leased line DSU to IR PRO

## **IR PRO FEATURES AND BENEFITS**

### **ISDN TA or regular modem Support**

The Network Device's WAN async port(s) can be used to connect to any ISDN TA or modem to another IP segment.

### **Proxy Router**

Unrestricted Internet access for everyone all the time!

### **Virtual Server (IP Mapping)**

Virtual server allows reverse NAT from WAN to LAN

### **IP Routing**

Segments your enterprise networks into workgroups

### **Asynchronous WAN port**

Can be configured as either Internet access, LAN-to-LAN or remote node dial-in service.

### **Remote access**

Remote client can directly be connected to the LAN by dialing into the asynchronous port.

### **DHCP Server**

Automatically assigns IP information to network users

### **DHCP Client**

Automatically gets IP information from ISP DHCP Server.

### **Filter**

Control incoming and outgoing data packets

### **Network Monitor Utility**

Allows the network administrator to view all incoming and outgoing packets, the status of connections and the specific connection Events

### **Multi-Platform based Configuration**

Windows-Based Configuration

Terminal Configuration

Remote Configuration

### **Firewall Protection**

Built-in NAT firewall guarantees network security

### **Frame Relay**

Supports Frame Relay protocol (T1, 617D, CCITT, ANSI)

### **RIP1/2**

Supports the Routing Internet Protocol (RIP1/2)

## **SOMEIR PRO FAQs**

Q : Does the IR PRO have firewall protection?

A : Built-in NAT firewall guarantees network security.

Q : What does the Virtual Server ( IP mapping ) do?

A : Virtual Server allows remote client access to your network via the Internet.

Q : What does IP Routing do?

A : It can segment your enterprise networks into workgroups and routes the IP packets amongst them.

Q : What does the Asynchronous WAN port do?

A : It can provide either Internet access or remote client service.

Q : What does the DHCP Client do?

A : It can automatically gets the IP information (including IP address, gateway IP, Subnet and DNS IP) from ISP' s DHCP server.

Q : What does the DHCP Server do?

A : It automatically assigns IP information to network users.

Q : What does Filter do?

A : It controls the incoming and outgoing data.

## THE NET-DEVICE UTILITIES

**The Net-Device utilities include :**

### **Net-Device Setup Wizard**

A step-by-step process that will let you input all the basic settings that are needed to configure your Network Device for general usage. All settings that are entered here will also be shown in their respective menus in the Net-Device Manager.

### **Net-Device Manager**

Net-Device Manager is the main program used to configure all the Settings of your Network Device.

### **Net-Device Monitor**

Net-Device Monitor is a multi-purpose utility that was designed for letting you know the status of your Network Device connection. It provides a step-by-step event monitor where by on each event you can point and click to bring up an on-line help screen that will advise you of any troubleshooting procedures that are needed.

### SETUP WIZARD

Setup wizard is a step-by-step process that will let you input all the basic settings that are needed to configure your Network Device for basic usage. All settings that are entered here will also be shown in their respective menus in Net-Device Manager.

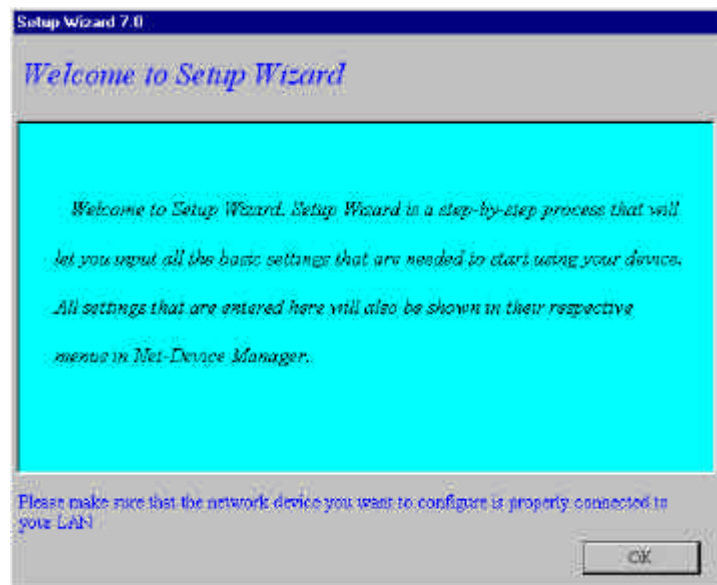
This manual assumes that you have a working knowledge of Microsoft Windows. Therefore, we will forego any introduction to Windows menu and operation Conventions.

Setup wizard will automatically start

After you have installed the Net-Device utilities, you will automatically be brought into setup wizard.

**To Run Setup Wizard from the Windows Start Menu**  
(after the Net-Device utilities has been installed on your PC)

- 1) Click **Start**
- 2) From the Program manager menu, choose **Program -> Net-Device**
- 3) and select **Setup Wizard** (see screen on the right)
- 4) Click **OK**

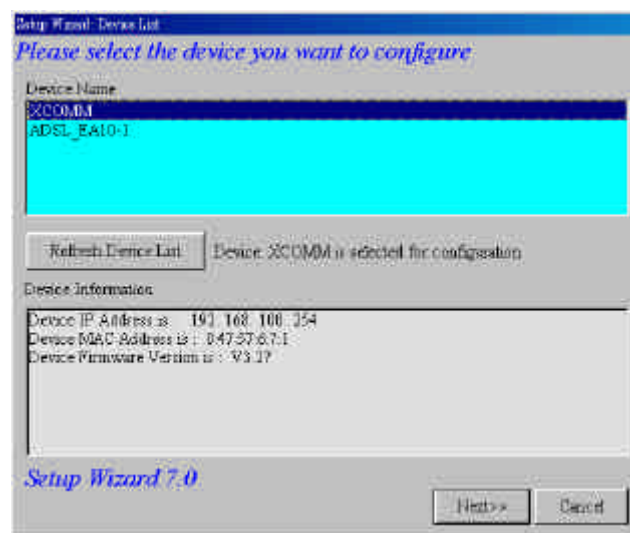


### Select the Device you wish to Configure

Setup wizard will automatically check your network for available Network Device and will list them in the **Device Name** section.

First select the device that you will be configuring from the **Device Name** section..

You can click the **`Refresh Device List`** button to update this list.



What if the device is not found displayed?

Click the **Refresh Device list** and see if the Network Device shows up, if not, please make sure that all cables are correctly plugged-in, connected and that the device is powered on.

Click **Next** to proceed to the next screen

### Set the device's IP address and name

The next thing you must do is to give your Network Device an IP address on your network. This is NOT the IP address from your ISP but the local internal LAN IP address.

The first two or three octets of every device or computer IP address on your network should be the same. Setup Wizard will help you by automatically detecting the IP address of your computer and set the first three octets for you. You need only decide on the last octet.

If you wish, you can also change the name of your Network Device to something else. This name is for your personal use only and can be anything you wish. If you are connecting a cable modem/ADSL to an ISP, the device name can act as your computer name, if your ISP requires you to input a computer name.

What is an IP address and how does it work?  
Please see the IP address entry in the Glossary.

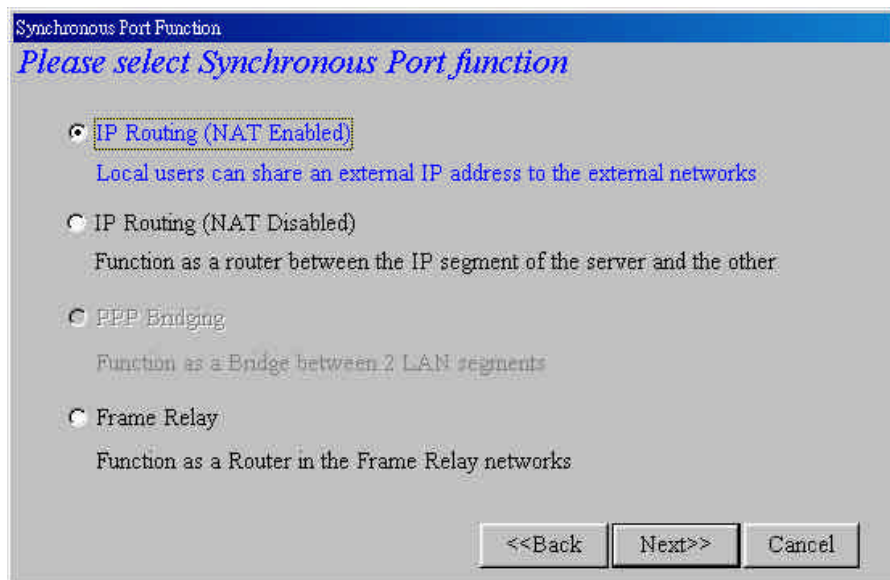
The screenshot shows a Windows-style dialog box titled "Setup Wizard: Device IP Address". The main text area contains the following instructions: "Please set the device's local LAN IP address and name", "Please give your new device an internal IP address on your network", "To help you out, Setup Wizard has determined that your computer's IP address is 192. 168. 100. 105 and has set the first three octets for you below.", "Please enter the last octet of the IP address.", and "You must choose an IP address that no other device on your network is using. If you would like more information on IP addresses please reference the glossary in your Net-Device user's manual." Below the text area, there are two input fields. The first is labeled "Set device's IP address as" and contains four small text boxes with the values "192", "168", "100", and "254". The second is labeled "The Device Name Will be Set to" and contains a text box with the value "XCOMM". At the bottom right of the dialog box are three buttons: "<<Back", "Next>>", and "Cancel".

Click **Next** to proceed to the next screen

### Port Function

Select the Port Function for the Synchronous Ports

You can configure it as either **IP Routing (NAT Enabled)**, **IP Routing (NAT Disabled)** or **Remote Access**.



#### Option 1) **IP Routing (NAT Enabled)**

The IP Routing Setting (NAT Enabled) allows the LAN users to access to the Internet by sharing just the external IP address of the synchronous port through the NAT mechanism.

#### Option 2) **IP Routing (NAT Disabled)**

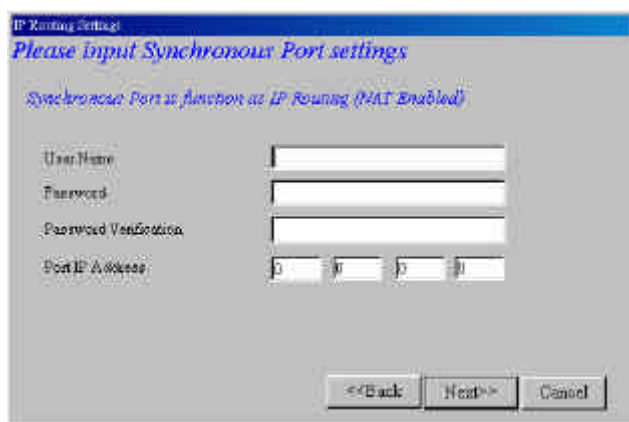
If you want to connect to another IP segment through the synchronous port, select the IP Routing Settings (NAT Disabled)

#### Option 3) **Frame Relay**

If XCOMM is connected to Frame Relay network, you have to select this option.

Click **Next** to proceed to the next screen

### Synchronous Port Settings



IP Routing Settings  
*Please Input Synchronous Port settings*  
*Synchronous Port is function as IP Routing (NAT Enabled)*

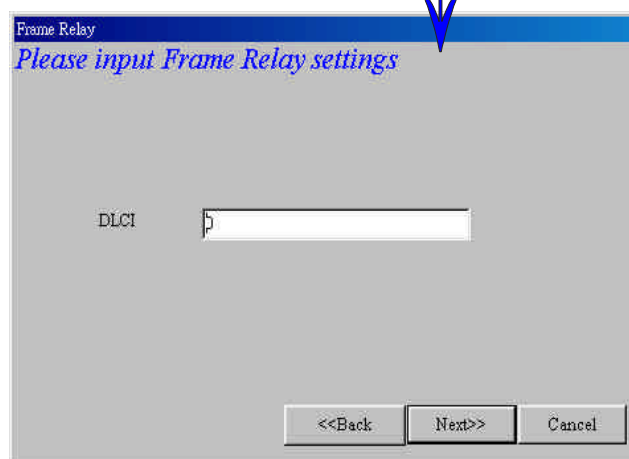
User Name:   
Password:   
Password Verification:   
Port IP Address:

<<Back Next>> Cancel

### Frame Relay Settings



Click

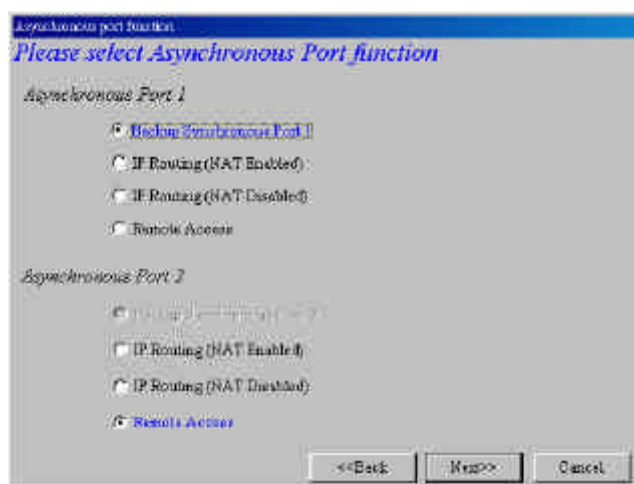


Frame Relay  
*Please input Frame Relay settings*

DLCI:

<<Back Next>> Cancel

### Asynchronous Port function



Asynchronous port function  
*Please select Asynchronous Port function*

*Asynchronous Port 1*

☒ [Function Synchronous Port 1](#)  
☐ IP Routing (NAT Enabled)  
☐ IP Routing (NAT Disabled)  
☐ Remote Access

*Asynchronous Port 2*

☐ [Function Synchronous Port 2](#)  
☐ IP Routing (NAT Enabled)  
☐ IP Routing (NAT Disabled)  
☒ Remote Access

<<Back Next>> Cancel

### IP Routing

Insert remote site(ISP or remote office)Info for IP Routing (Either NAT Enabled or Disabled)

If you select IP routing for the asynchronous port, The next thing you must do is input remote site (ISP or remote office) information which will be used to dial-up and login to your remote Server (ISP).

	Telephone	User Name	Password	Password Verification
Port 1				
Port 2				

Telephone Number : Enter your remote server(ISP) phone number.

User Name : Enter user name of your remote server(ISP) account.

Password : Enter the password of your remote server(ISP) account.

Password verification : Enter the password of your ISP account again to re-confirm.

If in your office or company you must dial a number to get an outside line (For example this is often the number `9` or `0`), you should enter the number plus a `w` which will instruct the XCOMM to wait until a dial-tone is received before dialling. For example the phone number 555-2323 which uses 9 to get an outside line would be entered as 9w555-2323. The XCOMM also support commas which function as delay variables. So our example number could also be entered as 9,,5552323. Each comma will provide around a 3-4 second delay.

Click **Next** to proceed to the next screen

### Remote Access

The remote user can dial-in to the asynchronous port to access the network as if the remote user is connected on the local network. It allows remote users to share files, receive all network services, even access the Internet.

If you select Remote Access for the Asynchronous Port, you have to input your Remote Access Settings

Now you must provide the remote access settings for the remote users :

You can use Local Client List or RADIUS Server for the remote users.

Option 1) Use the **Local Client List** (see above screen) The device allows you to input a maximum of 64 users.

**User name** : Enter the user name to authenticate the remote dial-in user.

**Password** : Enter the password to authenticate the remote dial-in user.

**Password Verification** : Re-type the password again for verification purposes.

**Callback Type** : You can set callback type for each remote client.

**No Callback** : The default setting for each user is NO Callback.

**Fixed Callback** : You can specify a fixed Callback Telephone number for the user. After PPP negotiation, the device will callback the telephone.

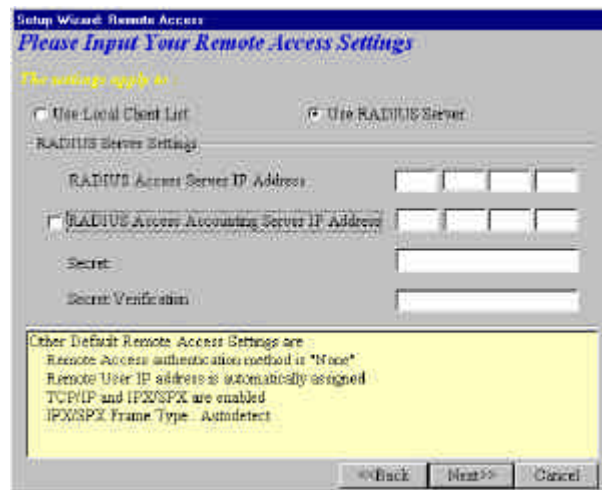
**Variable Callback** : The remote user can specify the callback telephone number for the device to callback.

Click **Next** to proceed to the next screen

## 2 - Remote Access

---

Option 2) Use RADIUS Server



### **RADIUS Access Server IP Address**

Enter the IP Address of the RADIUS Access Server

### **RADIUS Accounting Server IP Address**

Enter the RADIUS Accounting Server IP Address

**Note:** In most cases the RADIUS Access and Accounting Server are in the same Server (same IP address)

### **Secret**

Enter your Secret RADIUS code

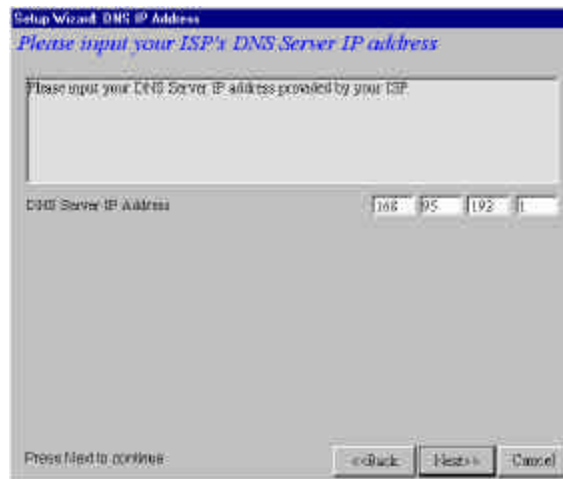
### **Secret Confirmed**

Enter your Secret RADIUS code again for verification purposes

Click **Next** to proceed to the next screen

### DNS IP

Input your ISP's DNS Server IP address

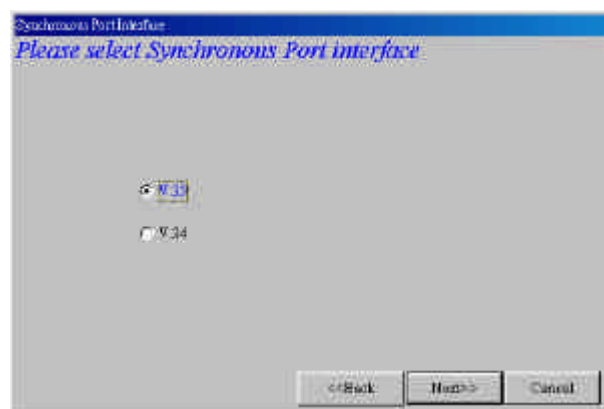


Enter the DNS Server IP address provided to you by your ISP. This information is usually provided to you with the information package given to you by your ISP. If you can't find your ISP's DNS Server IP address the easiest solution is probably to just give someone at your ISP a telephone call and ask them for the DNS Server IP address.

What is a DNS Server IP address?

Please see the DNS Server IP address entry in the Glossary.

### Synchronous Port interface

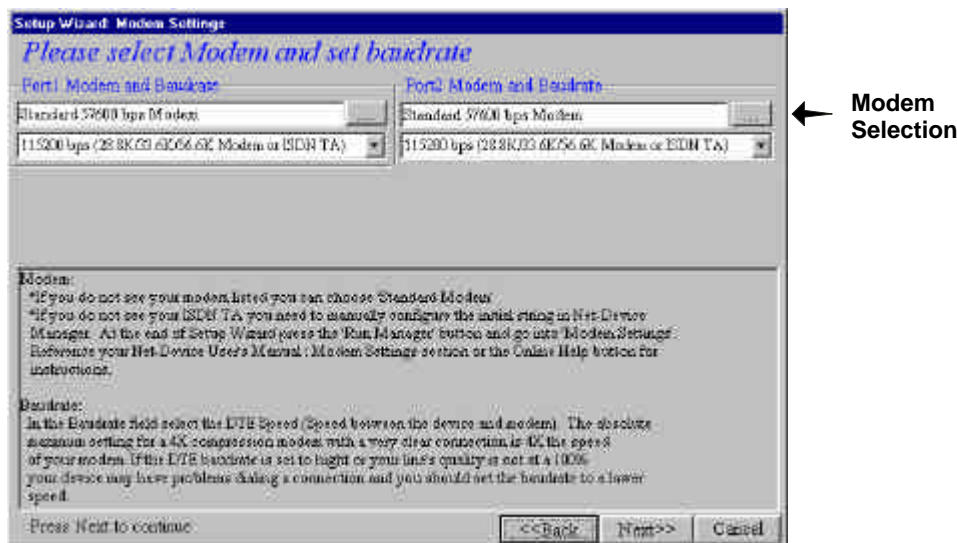


Click **Next** to proceed to the next screen

---

### Modem Settings

The last step is to enter the modem model that you are using and to set the DTE baudrate (i.e the speed of communication between the Network Device's Async port and your modem or ISDN TA). This is a very important setting and determines the communication between the asynchronous port of the Network Device and the modem.



#### Modem

You can click the `...` button to select your modem or ISDN TA. This setting will configure the initial string of the asynchronous port in the XCOMM, so that it will know how to communicate with your modem. If you are using an analog modem but do not see your modem in the modem selection list, in most cases the `Standard Modem` will work. Otherwise, read the modem or ISDN TA's user manual to set the Initial string and hang up string.

#### Baudrate

In the Baudrate field select the DTE speed (i.e the speed of communication between the asynchronous port of XCOMM and the modem) Normally this can be about 4 times the speed of your modem for DCE speed compression modems.

The maximum you should set the baudrate for a given port on your Network Device is 4 times the speed of your modem. If you set the baudrate too high, the Network Device may not be able to dial-up a connection.

**Note :** Some ISP connections and phone lines are not of the greatest quality, so the theoretical maximum speed is not attainable and you should set the baudrate at a lower speed.

Click **Next** to proceed to the next screen

## Finish

The Settings that you have just inputted will be summarized here. Please make sure that all settings are correctly inputted.

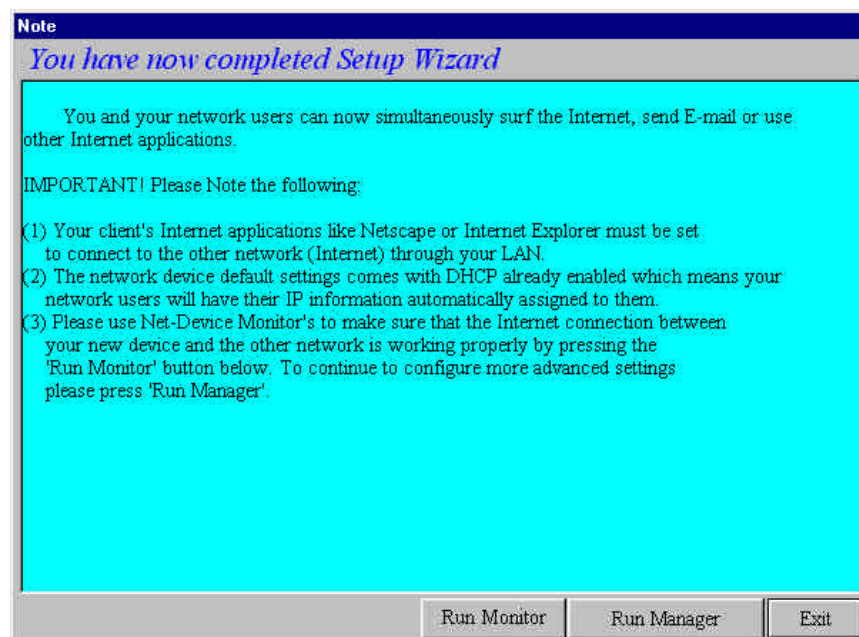
[illegible]

If you have configured a setting incorrectly, you can click on the **Back** button to return to the screen with the mistake and change it.

Press the **Finish** button to save your configuration to the Network Device.

### You have now completed the Setup Wizard

- 1) Press the **RUN MANAGER** button if you need to go to the Net-Device manager to configure more advanced settings.
- 2) Press the **Run Monitor** button if you don't need to configure anything else in Net-Device Manager and you want to use Net-Device Monitor's 'Test Connection' function to see if your Network Device can dial-up a connection with the settings that you have configured. Please see Section 4 - Net-Device Monitor for instructions.
- 3) Once you are running Monitor and the Test Connection has determined that your connection is okay, you should go to Setting up your Network Device Clients section and follow all the instructions carefully.



## NET-DEVICE MANAGER

Net-Device manager is the main program used to configure all the settings of your IR PRO.

### To Run Net- Device Manager

- 1) a) From your PC Desktop, click on the Net Device manager icon  
b) On the Windows 95/98/NT/2000 **Start** menu point to program, then to **Net Device Manger** and pick **Manager**.  
The main screen of the Net Device Manger is displayed as in figure 3.1
- 2) Select the device to be configured on the **Available Devices**, it will automatically check your network for any available devices and display it in the Available Devices box. Click the Refresh Device List Button to update this list.

#### Status:

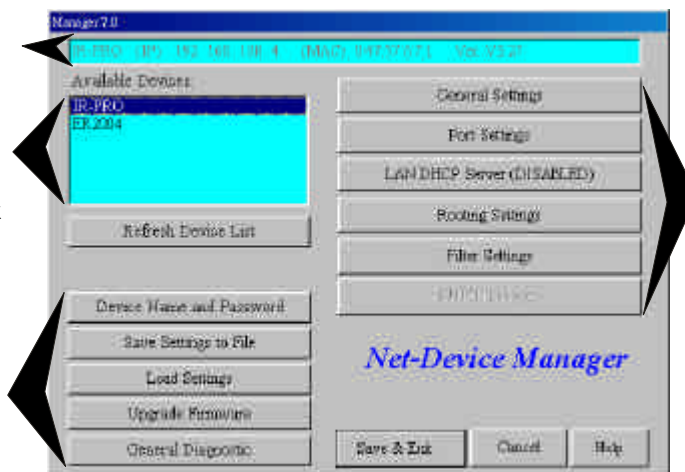
Displays the name of the Net Device, IP address, MAC address and version number

#### Avail Devices:

Displays all the available devices on the local network

#### Maintenance Buttons:

Supports the functions to change name/password, load/set settings, upgrade firmware and diagnose the device



#### Configure Buttons:

Provides advance configurations for the Net Device

Figure 3.1 Net-Device Manager's main screen

## General Settings

General Settings contain all the major settings for your Xcomm. It allows you to configure each external port in the Xcomm.

### LAN Ethernet Segment:

This is to configure your LAN port (RJ45). You input the IP address of your Xcomm in its LAN segment here.

### Synchronous Port:

Choose the protocol (PPP or Frame Relay) you would like to use for the Synchronous port.

### Asynchronous Port:

Choose the functions (Backup, IP routing or Remote Access) you would like for your Asynchronous Port.

The screenshot shows the 'General Settings' dialog box. It has a title bar 'General Settings'. The first section is 'LAN Ethernet Segment' with 'Device IP Address' set to 192.168.100.254 and 'Device Subnet Mask' set to 255.255.255.0. The second section is 'Synchronous Port' with 'PPP Routing' selected, 'HDLC' unselected, and 'Frame Relay' unselected. There is a 'Frame Relay LMI' field set to 10. The third section is 'Asynchronous Port' with 'Backup synchronous Port 1' selected, 'IP Routing' unselected, and 'Remote Access' unselected. There is a 'Remote Access' field set to 10. There are buttons for 'PPP Routing Settings', 'PPP HDLC Settings', and 'Remote Access Settings'. At the bottom, there are checkboxes for 'Enable IP Mapping' and 'Mapping Command Name', and 'OK', 'Cancel', and 'Help' buttons.

Figure 3.2 General Settings

### LAN Ethernet Segment

#### Device IP Address

The IP address of your Xcomm in its LAN segment is inputted here.

#### Device Subnet Mask

The Xcomm's subnet mask can usually be left as its default entry "255.255.255.0"

### 3 - General Settings

---

#### Synchronous Port

Select either **PPP** or **Frame Relay** as your synchronous port protocol.

#### PPP (Point to Point Protocol)

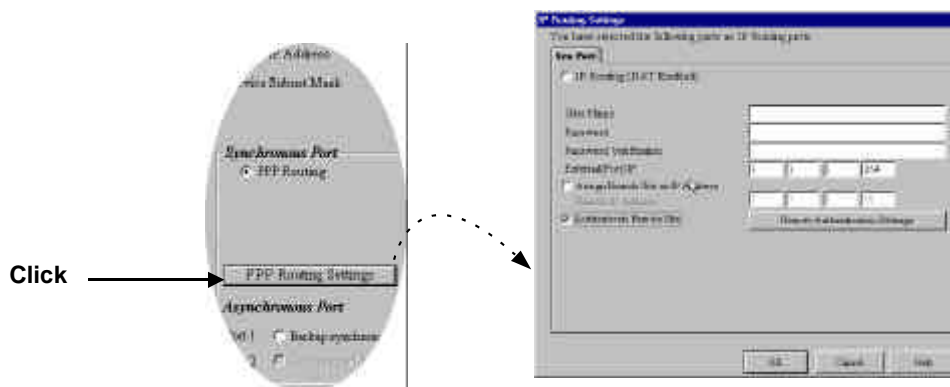


Figure 3.3 Synchronous Port PPP settings

If you select PPP as your synchronous port protocol you'll have to fill in the following:

##### IP Routing (NAT Enabled)

If NAT is enabled all local users will be firewall protected and will share one IP address through the port

##### User Name

Enter the user name to be authenticated by the remote site

##### Password

Enter the password to be authenticated by the remote site

##### Password Verification

Re-enter your password for verification purposes

##### External (Port) IP

Enter the fix IP address given by the remote site or 0.0.0.0 if it is to be automatically assigned by the remote site

##### Assign Remote Site an IP address

Check here if you want to specify an IP address for the remote site (Remote IP Address)

##### Authenticate Remote site

Check this box and click Remote Authentication Settings to specify how you would like to authenticate the remote users.

### 3 - General Settings

---

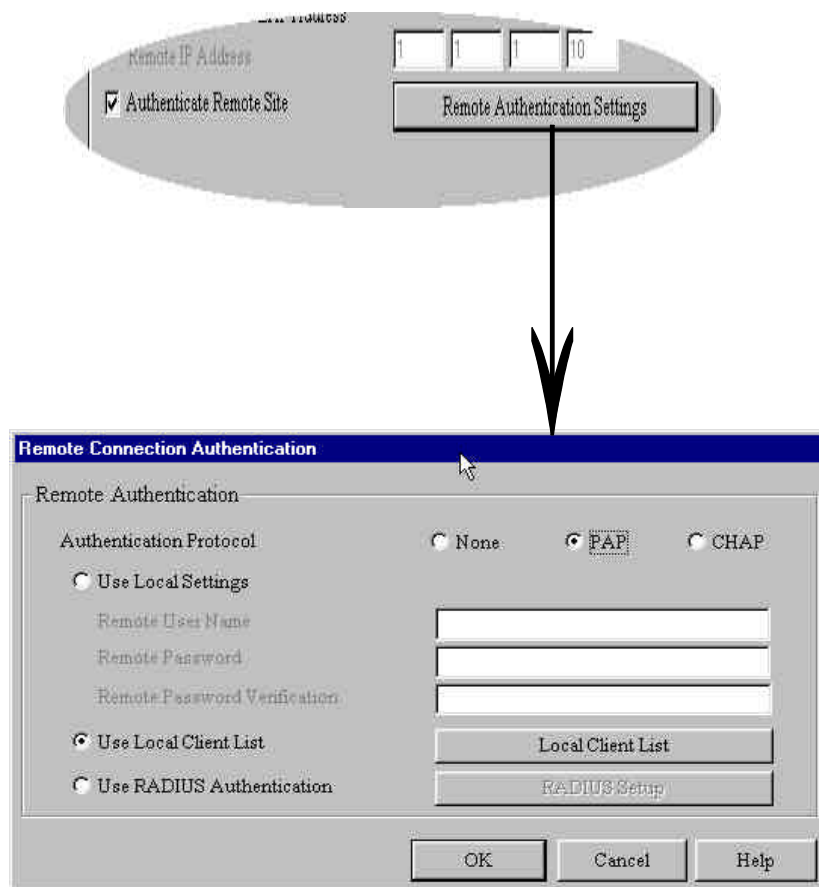


Figure 3.4

The client list used for LAN-to-LAN routing and the client list used for remote access is the same. The configuration that you enter here will apply to all of the remote access ports that you have configured for remote access, too.

### 3 - General Settings

---

#### Authentication Protocol:

- 1) None -No Authentication needed.
- 2) PAP -User Name and Password(encrypted) are transmitted over the network.
- 3) CHAP -DHCP sends a key which is used to encrypt the user name and password. The user name and passwords are transmitted over the network encrypted.

#### Authentication Method

If you choose one of the authentication protocols (PAP or CHAP), you'll then have to select one of the three authentication options listed below to authenticate the remote site.

##### Option 1) Use Local Setting

You can specify the user name and password needed to log-in. Therefore in order to log in all users must type the same user name and password which you inputted here.

##### Option 2) Use Local Client List.

The Local client list is a list of all Username/Password that can access your network from a remote site. When a remote user dials in to your Network Device, his/her user information (user name, password, callback...etc) will be validated by checking the user's information in this list. Your network device can save up to 64 users. Your network device comes with a default user called guest which has no password to login. For security reasons you should either delete the user guest or give it a password.

The screenshot shows a 'Client Configuration' window. On the left is a list box containing the name 'guest'. To the right, under 'Client Information', are four text input fields: 'User Name', 'Password', 'Password Verification', and a 'Callback Type' dropdown menu currently set to 'No Callback'. Below these fields is a checkbox labeled 'Assign a specific IP for this user', which is checked. To the right of the checkbox are four small text boxes for entering IP address segments. At the bottom, a note states 'The IP address set here will override the Port IP assignment'. On the far right are three buttons: 'OK', 'Cancel', and 'Help'. At the bottom center are two buttons: '< Back' and 'Next >'. The window has a blue title bar and a grey background.

Figure 3.5 Client Configuration Screen

### 3 - General Settings

---

#### Client Information

Fill in the following to add a new remote user to your Client list:

#### User Name

Specify the user name. Each name should not have more than 16 characters

#### Password

Specify the password which corresponds to the user name. Each password should not have more than 16 characters

#### Password Verification

Re-enter the password again for verification purposes

#### Callback Type

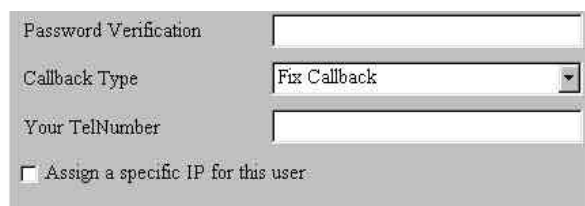
Callback Type refers to the function whereby a remote client dials in to your Network Device and purposely disconnects. The Network Device then calls back the remote client. This is mainly used for control purposes. The network devices Remote Authentication Setting comes with three callback options, they are listed below

##### 1) No Callback

If NO Callback is selected, the network device will not allow any callback services. This is the default settings.

##### 2) Fixed Callback

If Fixed Callback is selected, the remote user is allow the callback service, but the callback phone number is restricted to a fixed phone number. This phone number is defined in the **Your TelNumber** field.



The screenshot shows a web-based configuration form for Remote Authentication. It contains the following fields and controls:

- Password Verification:** A text input field.
- Callback Type:** A dropdown menu with "Fix Callback" selected.
- Your TelNumber:** A text input field.
- Assign a specific IP for this user:** A checkbox that is currently unchecked.

##### 3) Variable Callback

If the Variable Callback is selected, the remote user will be allowed to have the callback service and will also be able to specify the callback phone number each time he/she dials up.

### 3 - General Settings

---

#### Assign a specific IP address for this user

If you would like to have an IP address assigned for this specific user, first enable this setting and input an IP address for this user. NOTE: this IP address will always be used for this specific user and will override the **Assign Remote Site an IP address** field.

Click **Add** when you've filled out all the client information and you want to add the new user to the Local Client List

#### Option 3) RADIUS Authentication

Choosing RADIUS configuration will allow you to use the user information (user name, password, IP address.. Etc.) stored on a separate RADIUS server on the network. Basically a RADIUS server is a user database that records the network setting which can keep track of accounting information as well as dial-in privileges. When a remote user dials in to your network device, the user's information will be validated by checking the user's information stored in the network RADIUS server. RADIUS configuration is generally used by large companies or by ISPs (Internet Service Provider) to keep track of remote users.



Figure 3.6 Async Port - Remote Access Authentication - RADIUS

#### **RADIUS Access Server IP Address**

Enter the IP Address of the RADIUS Access Server

#### **RADIUS Accounting Server IP Address**

Enter the RADIUS Accounting Server IP Address

**Note:** In most cases the RADIUS Access and Accounting Server are in the same server (same IP address)

#### **Secret**

Enter your Secret RADIUS code

#### **Secret Confirmed**

Enter your Secret RADIUS code again for verification purposes

### 3 - General Settings

---

#### Frame Relay

If you select Frame Relay as your synchronous port protocol, you'll need to fill in the following:

**DLCI** (Data Link Connection Identifier)  
Input your DLCI number, given to you by your Service Provider and then click **ADD** (click **Delete** to delete the DLCI)

#### Advanced Setting

##### Link Manager Protocol

XCOMM supports ANSI T1-617D, LMI and ITU-T ANNEXA management protocol. You have to select the management Protocol your ISP supports. Default is ANSI T1-617D.

##### Use IETF(RFC1490)

RFC1490 is the default protocol for carrying network internet traffic over a frame relay backbone.

#### DLCI Settings

##### DLCI

Input the DLCI value assigned by your ISP.

##### Port IP Address

Input the IP Address of this port.

##### Port IP Netmask

Input the IP netmask of the port.

##### Remote IP Address

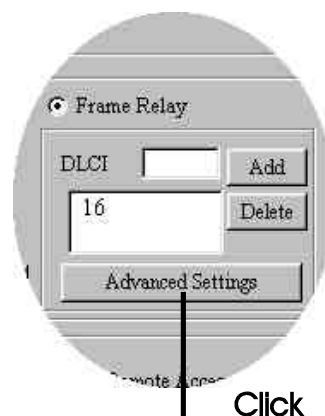
Input the remote site IP address.

##### Remote IP Netmask

Input the remote site IP Netmask.

##### Information Rate

Select the Information Rate of this DLCI Link.



Click

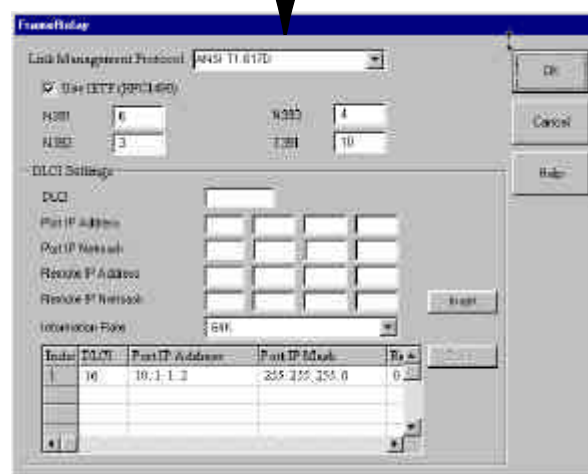
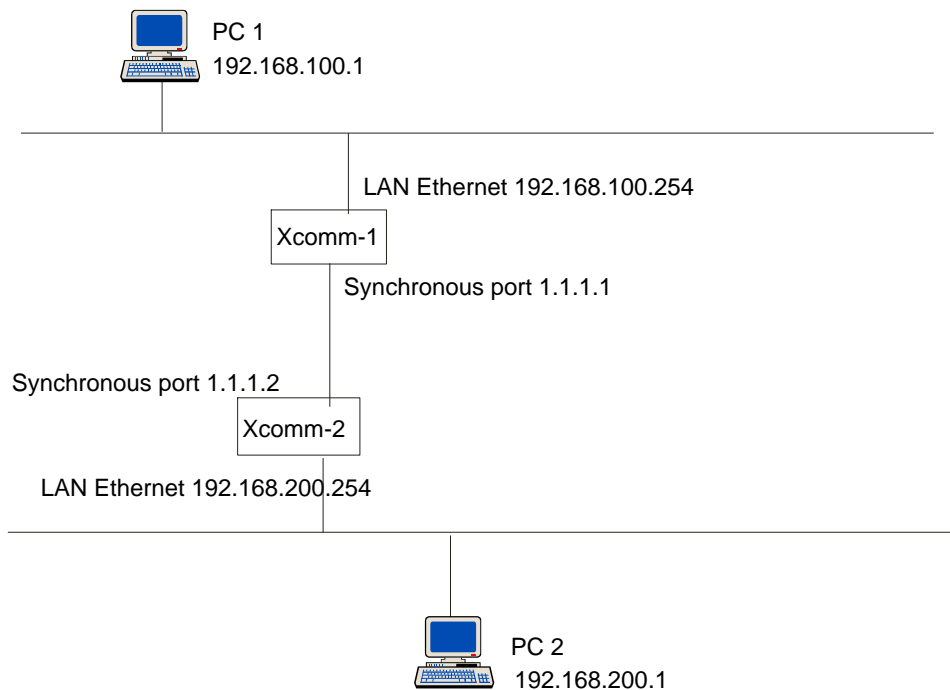


Figure 3.7 Synchronous Port - Frame Relay Advance Settings

### 3 - General Settings

---



#### **XCOMM1**

**DLCI = 16**

**Port IP = 1.1.1.1**

**Port IP Netmask = 255.255.255.0**

**Remote IP = 192.168.200.254**

**Remote Netmask = 255.255.255.0**

#### **XCOMM2**

**DLCI = 17**

**Port IP = 1.1.1.2**

**Port IP Netmask = 255.255.255.0**

**Remote IP = 192.168.100.254**

**Remote Netmask = 255.255.255.0**

## Asynchronous Port

Select which function (**Backup**, **IP routing** or **Remote Access**) you would like to set for the Asynchronous Port



## Backup Synchronous

If the sync port goes down, this function will instruct the async port(s) to establish a connection so that your network is always connected

### Tel number

Enter Remote site's telephone number

### User Name

Enter the user name to be authenticated by the remote site

### Password

Enter the password to be authenticated by the remote site

### Password verification

Re-enter password for verification purposes

### External (Port) IP

Enter the fix IP address (given by the remote site) or else 0.0.0.0 if it is to be automatically assigned by the remote site

### Assign Remote Site an IP Address

Check here if you want to specify an IP address for the remote site. (Remote IP address)

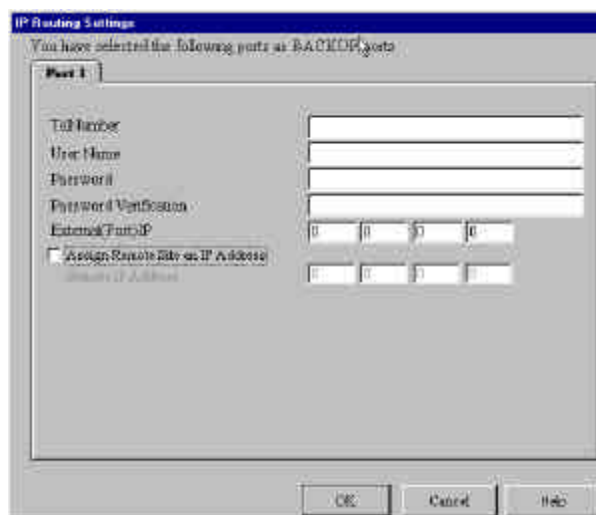
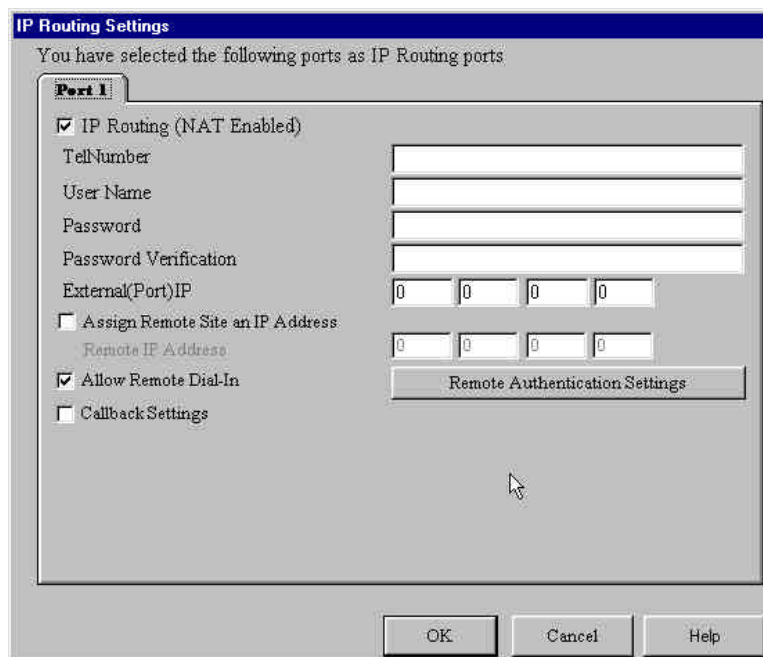


Figure 3.8 Back up Synchronous Port

#### IP Routing (PPP Settings)



The image shows a Windows-style dialog box titled "IP Routing Settings". At the top, it says "You have selected the following ports as IP Routing ports:". Below this is a tab labeled "Port 1". Inside the tab, there are several settings: a checked checkbox for "IP Routing (NAT Enabled)", followed by text labels for "TelNumber", "User Name", "Password", and "Password Verification", each with a corresponding text input field. Below these is a label "External(Port) IP" with a four-digit numeric input field (0 0 0 0). Then there is an unchecked checkbox for "Assign Remote Site an IP Address", followed by a label "Remote IP Address" with another four-digit numeric input field (0 0 0 0). Below that is a checked checkbox for "Allow Remote Dial-In" and an unchecked checkbox for "Callback Settings". A button labeled "Remote Authentication Settings" is positioned to the right of the "Allow Remote Dial-In" checkbox. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

Figure 3.9 IP Routing setting

##### **IP Routing (NAT Enabled)**

If NAT is enabled all local users will be firewall protected and will share one IP address through the async port

##### **Tel number**

Enter remote site telephone number

##### **User Name**

Enter the user name to be authenticated by the remote site

##### **Password**

Enter the password to be authenticated by the remote site

##### **Password verification**

Re-enter password for verification purposes

##### **External (Port) IP**

Enter the fix IP address (given by the remote site) or else 0.0.0.0 if it is to be automatically assigned by the remote site

##### **Assign Remote Site an IP Address**

Check here if you want to specify an IP address for the remote site. (Remote IP address)

### 3 - General settings

---

## Allow Remote Dial-In

### Remote Authentication Settings

The settings here allows you to specify how you would like to authenticate the remote dial-in user.

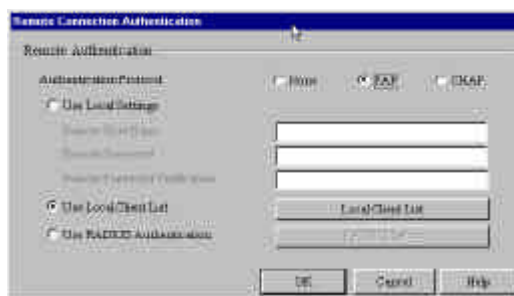


Figure 3.10 Async Port - Remote Access Authentication

### Remote Authentication

#### Authentication Protocol

- 1) None - No Authentication required
- 2) PAP - User Name and Password are transmitted over the network
- 3) CHAP - User Name and Password are transmitted over the network encrypted

### Authentication Method

If you choose one of the authentication protocols (PAP or CHAP). You'll then have to select one of the three authentication options listed below to authenticate the remote site.

#### Option 1) Use Local Setting

You can specify the user name and password needed to log-in. Therefore in order to log in all users must type the same user name and password which you specify here.

### 3 - General settings

---

#### Option 2) Use Local Client List

The Local client list is a list of all Username/Password that can access your network from a remote site. When a remote user dials in to your Network Device, his/her user information (user name, password, callback...etc) will be validated by checking the user's information in this list. Your network device can save up to 64 users. Your network device comes with a default user called guest which has no password to login. For security reasons you should either delete the user guest or give it a password.

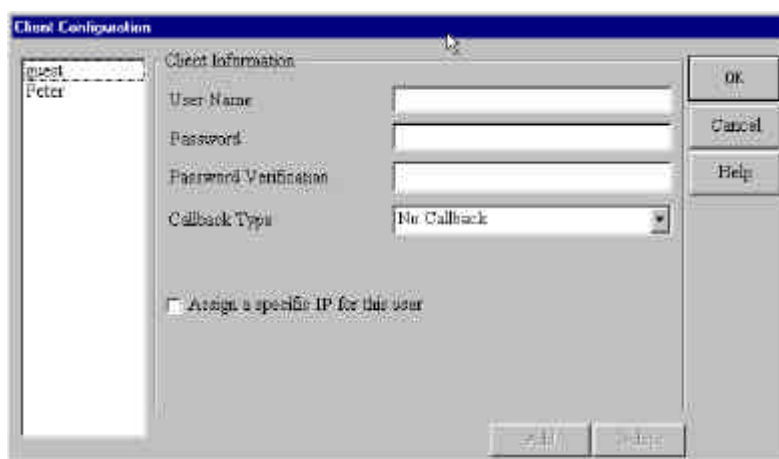


Figure 3.11 Async Port - Remote Access Authentication- Local Client List

#### Client Information

Fill in the following to add a new remote user to your client list:

##### User Name

Specify the user name. Each name should not have more than 16 characters

##### Password

Specify the password which corresponds to the user name. Each password should not have more than 16 characters

##### Password Verification

Re-enter the password again for verification purposes

##### Callback Type

Callback Type refers to the function whereby a remote client dials in to your Network Device and purposely disconnects. The Network Device then calls back the remote client. This is mainly used for control purposes. The network device comes with three callback options, they are listed below

### 3 - General settings

---

#### 1) No Callback

If NO Callback is selected, the network device will not allow any callback services. This is the default settings.

#### 2) Fixed Callback

If Fixed Callback is selected, the remote user is allowed the callback service, but the callback phone number is restricted to a fixed phone number. This phone number is defined in the **Your TelNumber** field variable.



The screenshot shows a configuration window for a user. It includes a 'Verification' field, a 'Callback Type' dropdown menu set to 'For Callback', and a 'Your TelNumber' text input field. Below these fields is a checkbox labeled 'Assign a specific IP for this user'.

#### 3) Variable Callback

If the Variable Callback is selected, the remote user will be allowed to have the callback service and will also be able to specify the callback phone number each time he/she dials up.

### Assign a specific IP address for this user

If you would like to have an IP address assigned for this specific user, first enable this setting and input an IP address for this user. NOTE: this IP address will always be used for this specific user and will override the Assign Remote Site an IP address in IP previous settings.



The screenshot shows a configuration window with a checked checkbox labeled 'Assign a specific IP for this user'. Below the checkbox is a text input field for the IP address, followed by four small square buttons. A note at the bottom states: 'The IP address set here will override the Port IP assignment'.

Click Add when you've filled out all the client information and you want to add the new user to the Local Client List

### 3 - General settings

---

#### Option 3) RADIUS Authentication

Choosing RADIUS configuration will allow you to use the user information (user name, password, IP address.. Etc.) stored on a separate RADIUS server on the network. Basically a RADIUS server is a user database that records the network setting which can keep track of accounting information as well as dial-in privileges. When a remote user dials in to your network device, the user's information will be validated by checking the user's information stored in the network RADIUS server. RADIUS configuration is generally used by large companies or by ISPs (Internet Service Provider) to keep track of remote users.

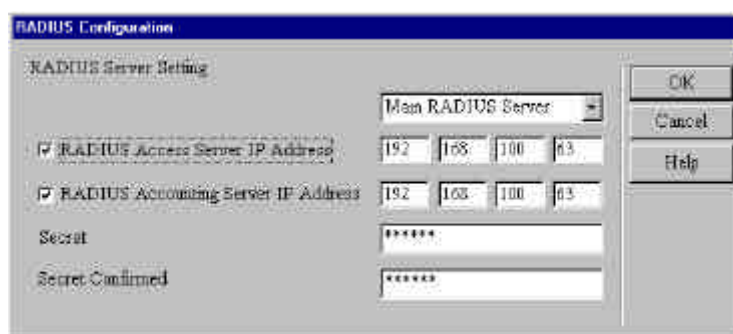


Figure 3.12 Async Port - Remote Access Authentication - RADIUS

#### **RADIUS Access Server IP Address**

Enter the IP Address of the RADIUS Access Server

#### **RADIUS Accounting Server IP Address**

Enter the RADIUS Accounting Server IP Address

**Note:** In most cases the RADIUS Access and Accounting Server are in the same server (same IP address)

#### **Secret**

Enter your Secret RADIUS code

#### **Secret Confirmed**

Enter your Secret RADIUS code again for verification purposes

## Remote Access

### IP Assigned Method for Remote Clients



#### Assign an IP address automatically

The network device's DHCP will assign the remote site an IP address if the DHCP server function of the Net Device is enabled. Otherwise the Net Device will automatically search for a DHCP server in its network and request the server an IP address for the remote client

#### Assign an IP Address Manually

You can choose an IP address for the remote site

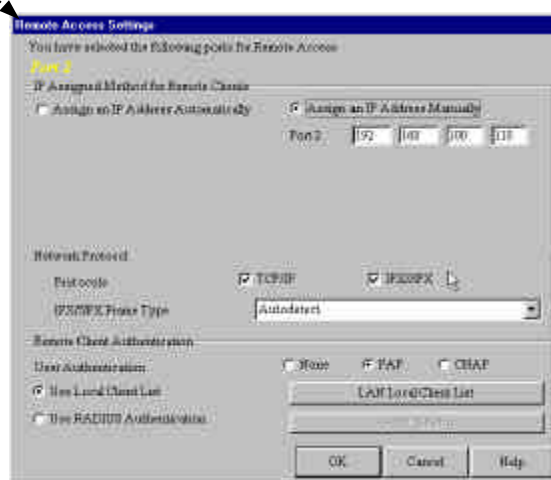


Figure 3.13 Asynchronous Port - Remote Access

### Network Protocol

Protocols	TCP/IP	IPX/SPX
-----------	--------	---------

Here you can select which protocols you would like to enable for the dial in service.

If you connect a remote site to a Window NT server, at least a TCP/IP protocol or an IPX/SPX protocol must be enabled. The default has both TCP/IP and IPX/SPX enabled.

If you connect a remote site to a NetWare server you must enable the IPX/SPX protocol.

### IPX/SPX Frame Type

The Xcomm can automatically detect what kind of IPX/SPX frame type you are using. If you would like to manually set the frame type, use the drop down list to choose which type.

### Remote Client Authentication

Remote Authentication Settings allows you to specify how you would like to authenticate the remote users.

### 3 - General settings

---

#### Enable IP Mapping

If NAT is enabled for a particular port, that port is firewall protected. However, the Enable IP Mapping function allows clients on the Internet to access your LAN via the Internet. For example, you can use the IP Mapping function to access an FTP server on your LAN via your ISP Internet connection.

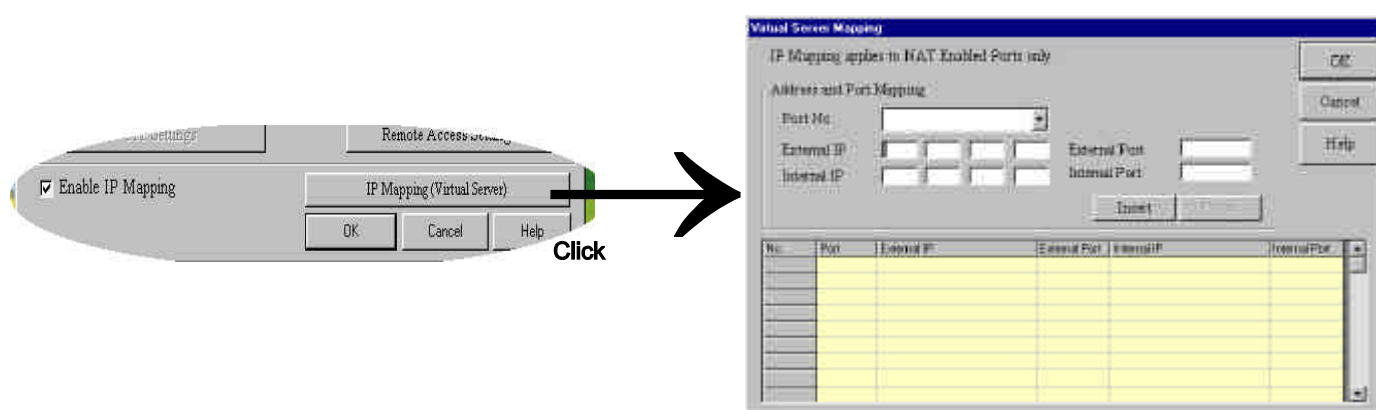


Figure 3.14 Enable IP Mapping screen.

To enable the IP Mapping function click the Enabled circle.

For each service that you want to setup:

- 1) Select which protocol (Either TCP, UDP or All) the service uses. Most services use TCP (WWW, FTP, E-mail etc..).
- 2) Enter your IP address supplied by your ISP in the External IP field. If your ISP gives you a dynamic IP address, you can set this as 0.0.0.0. Your network device will then use whatever dynamic IP address your ISP gives it as the external IP.

### 3 - General Settings

---

#### External Port

3) Enter the TCP/IP port number for the service that you will be using for IP mapping. Some common TCP/IP port numbers are listed below.

WWW Port# = 80  
FTP Port# = 20 or 21  
SMTP Port# = 25  
POP3 Port# = 110

More information on port numbers, please visit the link below.  
[Http://www.metadigm.co.uk/tech/portnum.txt](http://www.metadigm.co.uk/tech/portnum.txt)

If you would like to map all services for this external IP address into a computer on your LAN you can enter the port number 0. This means that whenever anyone accesses your external IP address they will be automatically be "mapped" into the internal computer that you specify regardless of what port number they are using.

#### Internal IP

4) Enter the IP address of the server that you want the external IP address to map to.

#### Internal Port

5) Enter the port number for the service that you will be using for this IP mapping.

Press the **Insert** button to insert this mapping.

A limitation of the IP Mapping function is that you can only have/specify one port service on your local network. For example, If you map an external IP (168.95.1.3) to an Internal IP (192.168.2.254) eg- www.server. Then only that internal IP address in your local network can serve as a www.server for the external IP address.

Note 1 : The IP mapping is only available when the device's NAT is enabled.  
Note 2 : IP mapping is most suitable for a fixed IP address.

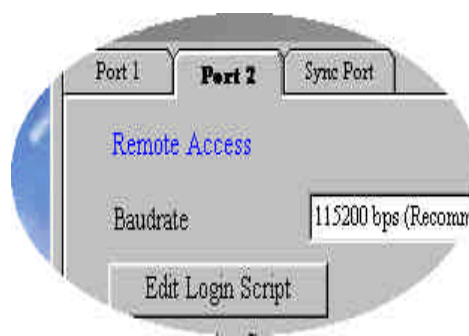
## 3 - Port Settings

---

### *Port Settings (Async Port)*

If the Async Port function is set as IP routing, the port setting for IP routing will be displayed

If the Async port function is set as Remote Access, the port setting for Remote Access will be displayed



Baudrate  
Please select the device for your port DTE speeds.

The maximum you should set the baudrate for a given port on your Network Device is 4 times the speed of your modem. If you set the baudrate too high your network device may not be able to dial-up a connection. For example if you have a 14.6Kbps modem, the highest you should set the baudrate is 57.6Kbps. You should also be aware that since some ISP connections and phone lines are not of the greatest quality, this theoretical maximum speed is not attainable and you should set the baudrate at a lower speed.

The modem string setting instructs each serial port on your network device the basic communication instructions needed to communicate with the attached modem or ISDN TA.

### 3 - Port Settings

---

#### Edit Login Script (See Figure 3.13)

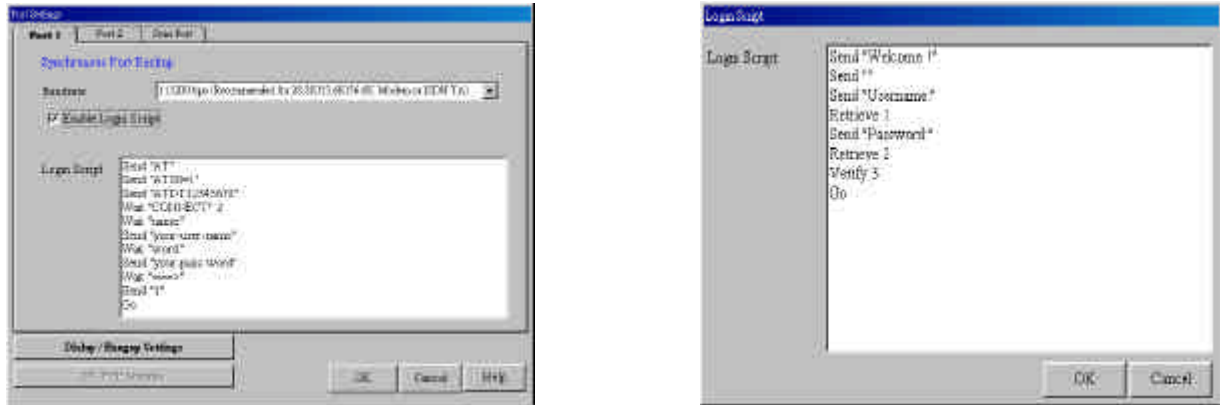


Figure 3.13 Login Script screen.

Learn the login script commands available to you.

#### Example Commands

- |                               |  |
|-------------------------------|--|
| <b>- Send and SH commands</b> | <b>Result</b>  |
| Send `ATZ`                    | Resets Modem   |
| Send `ATDT 888-1234`          | Dials phone number 888-1234  |
| Send `PeterMiles`             | Types `PeterMiles` at ISP interface  |
| SH `1234`                     | Types `1234` at ISP interface but displays<br>**** in Net-Device Monitor display to hide<br>password.  |
| Send ``                       | Types Enter key at the ISP Internet<br>(Important for ISPs like Compuserve)  |
| <b>- Wait commands</b>        |  |
| Wait 5                        | Modem will wait for 5 seconds before<br>going to next command.   |
| Wait `CONNECT`                | Modem will wait for `CONNECT` to come<br>onto screen before going to next command.   |
| Wait `CONNECT` 6              | Modem will wait for `CONNECT` to come<br>onto screen before going to next command.<br>If connect does not come onto screen,<br>modem will go back to line 6 of Login Script. |
| <b>- Other commands</b>       |  |
| Go                            | Begins PPP   |
| Jump4                         | Will go back to command line 4   |
| Hangup                        | Hangs up Modem   |

### Writing a login script for Remote Access

#### Step A)

For **Remote Access**, the device will act as the server side..

**Send `Welcome`** will display `Welcome` to remote site.

**Send ` `** sends an Enter (Carriage Return + Line Feed) to the remote site.

**Send `Username`** will display `User Name` to the remote site.

**Retrieve 1** will wait for the remote site to input user name, and use it as the user name in the PPP authentication.

**Retrieve 2** will wait for the remote site to input password, and use it as the password in the PPP authentication.

**Verify 3** will indicate the device to jump to login script line number 3 if PPP authentication fails.

**Go** means start PPP protocol.

#### Step B) Get Login Script Information

Because every ISP has a different interface screen when logging in, you must check to see when and how your ISP requests information from you. Your network device uses PPP user service so when logging into your ISP, please find out the selection for PPP service.

**NOTE** : You can get your ISP interface log-in screen by doing a simple dial-up connection using the Dial-up Networking utility in Windows 95. Your Windows 95 **Dial-up Networking** folder is located in the **My Computer** icon.

#### Step C) Make your login script

Below are two examples of the login scripts for our example ISP. On the left is the actual inputted login script. On the proceeding page we highlighted the important parts that you needed to note which are again highlighted below where they are used.

#### Example 1 : Script for Normal Reliable ISP

#	Login Script	Meaning of Each Login Script Command
1	<b>Send `ATZ`</b>	Rests Modem
2	<b>Send `AT S0 = 1`</b>	Sends initial string ` AT S0 = 1` to modem
3	<b>Send `ATDT 888-1234`</b>	Dial phone number 888-1234
4	<b>Wait `CONNECT`</b>	Waits for ISP to send reply `CONNECT`
5	<b>Wait `username:`</b>	Waits for ISP to send reply `username`
6	<b>Send `PeterMiles`</b>	Sends the user name `PeterMiles` to ISP
7	<b>Wait `password`</b>	Waits for ISP to send reply `password`
8	<b>SH `1234`</b>	Sends password `1234` to ISP
9	<b>Wait `====&gt;`</b>	Waits for ISP to send reply `====>`
10	<b>Send `1`</b>	Selects option 1 (PPP) for this ISP
11	<b>Go</b>	Starts PPP mode

#### Example 2 : Script for unreliable ISP (Redial until connected)

#	Login Script	Meaning of Each Login Script Command
1	Send `ATZ`	Resets modem
2	Send `AT S0 = 1`	Sends initial string `AT S0 = 1` to modem
3	Send `ATDT 8881234`	Dials phone number 888-1234
4	Wait `CONNECT` 2	Wait for ISP to send reply `CONNECT`. If not will go back to line 2 to re-dial.
5	Wait `username:` 12	Waits for ISP to send reply `username`. If no response will go to line 12
6	Send `PeterMiles`	Sends the username `PeterMiles` to ISP
7	Wait `password`	Waits for ISP to send reply `password`
8	SH `1234`	Sends password `1234` to ISP
9	Wait `====>`	Waits for ISP to send reply `====>`
10	Send `1`	Selects option 1 (PPP) for this ISP
11	Go	Starts PPP mode
12	Hangup	Hangs up Modem

#### Example 3 : Script for unreliable ISP (2nd ISP backup)

#	Login Script Example 2	Meaning of Each Login Script Command
1	Send `ATZ`	Resets modem
2	Send `AT S0 = 1`	Sends initial string `AT S0 = 1` to modem
3	Send `ATDT 8881234`	Dials phone number 888-1234 (ISP #1)
4	Wait `CONNECT` 12	Waits for ISP to send reply `CONNECT`. If not will go to line 12 for ISP #2
5	Wait `username:` 12	Waits for ISP to send reply `username`. If no response will go to line 12 for ISP #2
6	Send `PeterMiles`	Sends the username `PeterMiles` to ISP
7	Wait `password`	Waits for ISP to send reply `password`
8	SH `1234`	Sends password `1234` to ISP
9	Wait `====>`	Waits for ISP to send reply `====>`
10	Send `1`	Selects option 1 (PPP) for this ISP
11	Go	Starts PPP mode (Rest of script ignored)
12	Hangup	Hangs up modem
13	Send `AT S0 = 1`	Sends initial string `AT S0 = 1` to modem
14	Send `ATDT 8885678`	Dials phone number 888-5678 (ISP #2)
15	Wait `CONNECT` 23	Waits for ISP to send reply `CONNECT`. If not received will go to line 23.
16	Wait `username:` 23	Waits for ISP to send reply `username`. If no response will go to line 23.
17	Send `Jamie`	Sends the user name `Stephen` to ISP
18	Wait `password`	Waits for ISP to send reply `password`
19	SH `5678`	Sends password `5678` to ISP
20	Wait `====>`	Waits for ISP to send reply `====>`
21	Send `1`	Selects option 1 (PPP) for this ISP
22	Go	Starts PPP mode (Rest of script ignored)
23	Hangup	Hangs up modem
24	Jump 2	Goes back to line 2 to re-dial ISP #1

### Modem String Settings

#### Select Modem and Modem String Setting

The most important modem string is the initial string because your network device uses it to establish communication with your modem or ISDN TA. The modem initial string displayed here was configured automatically when you selected your modem or ISDN TA in the Setup Wizard. If your modem is not listed in the Modem Selection List, the Standard Modem selection will work with most modems.

#### ISDN Settings **!!! Important !!!**

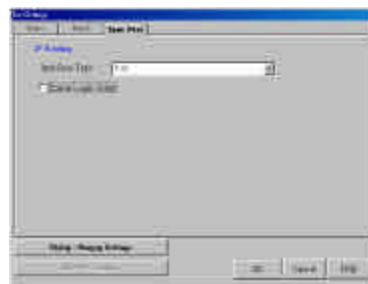
Unfortunately, unlike most modems, ISDN initial strings vary between different ISDN TAs and there is no "Standard ISDN TA" initial string. If your ISDN TA is not listed in the modem selection list you must find out what your ISDN TA initial string is. Your ISDN TA's initial string should be listed in your ISDN TA user's manual. There are probably many initial strings listed for your ISDN TA. The one you are looking for is Asyn-to-Syn PPP (Asynchronous to Synchronous PPP). You can enter this initial string if you would like to use only one channel of your ISDN TA. If you would like to bundle both channels of your ISDN TA together, you need to use a different initial string called Multilink-PPP. For example, the initial strings for a Zyxel Omninet ISDN TA are:

- 1) ATB40: Asyn-to-Syn PPP initial string
- 2) AT&J3: Multilink-PPP initial string

You should also verify that your ISDN TA supports the Dial-up string ATDT. Most ISDN TAs will support ATDT and usually the rest will support ATD or ATDI.

Please also note that to bundle the two channels of your ISDN TA together, you must enter the two phone numbers in the Telephone Number field of the General settings menu.

#### Interface Type (Synchronous port only)



### 3 - Port Settings

---

#### Dial-up / Hang-up Settings (Click **Dial-up/Hang-up Settings** on Port Settings)

The Dial-up/Hang-up settings allows you to specify your connection time (idle timeout or auto reconnect) and the number of times to attempt to connect (if connection can not be established)

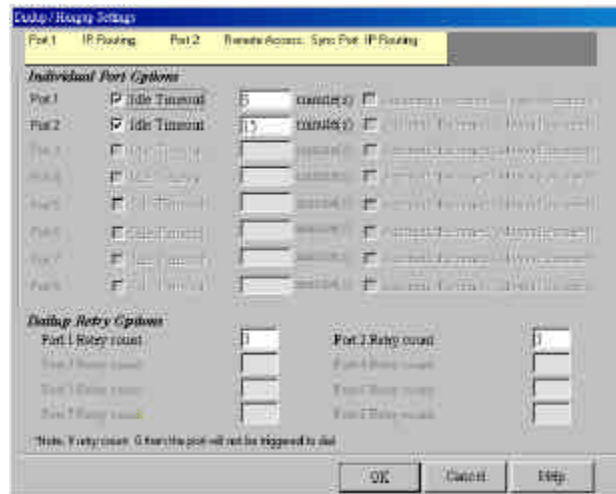


Figure 3.14 Dial-up / Hang-up Setting screen.

#### **Individual Port Options**

Individual Port Options lets you set the idle-timeout function for each serial port of your Network Device. Here you can set the number of minutes you wish to allow a connection to stay idle before disconnecting. Default Idle timeout for IP Routing is 5 minutes, and default Idle timeout for remote access is 30 minutes.

If you un-check the idle-timeout, once a client establishes a connection, the connection will be maintained until you turn off your modem, unplug your network device or use the Terminate Connection function in Net-Device Monitor.

The Automatic Reconnect (Always connect) essentially maintains your connection (e.g. Idle time out = infinite). If the connection is disconnected For some reason, it will automatically attempt to reconnect.

**Dial-up Retry Options** - allows you to specify the number of times the Network Device should attempt to establish a connection.

If the retry count is 0, the device will not dial-out to connect to the remote site.

Automatic Reconnect will override the retry count setting if retry count is set to 0.

### 3 - Port Settings

---

**ML-PPP** (Click **ML-PPP** on fig 3.15.1 and fig 3.15.2)

ML-PPP is a protocol that will widen your bandwidth through connecting two or more lines. You can therefore connect two modems to your two ports and have double the bandwidth. ML-PPP will bundle the packets together as though the two connections is one larger bandwidth connection.



Figure 3.15.1 Use ML-PPP

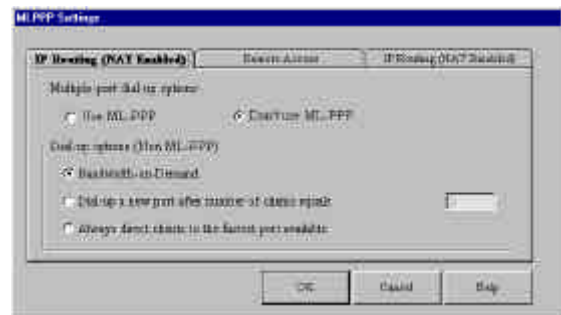


Figure 3.15.2 Don't Use ML-PPP

#### **Use ML-PPP (fig 3.15.1)**

Select one of the following selections:

##### **Bandwidth on Demand**

When the traffic becomes too heavy, the bandwidth on Demand function will trigger the second line using ML-PPP.

##### **Dial-up a new port after number of clients equal**

The Network Device will dial a new port when the number of users equals or exceeds the number you specify

##### **Always use ML-PPP**

The Network Device will always use the ML-PPP protocol no matter how many users are using the connections.

#### **Don't use ML-PPP (fig 3.15.2)**

Select one of the following selections:

##### **Bandwidth on Demand**

When the traffic becomes too heavy, this function will see if there are other routes to relieve the load e.g another connection to an ISP (without ML-PPP)

##### **Dial-up a new port after number of clients equal**

The Network Device will dial a new port when the number of users equals or exceeds the number you specify

##### **Always direct clients to the fastest port available**

The Network Device will see which port is not so busy and direct the clients to that port.

### 3 - Port Settings

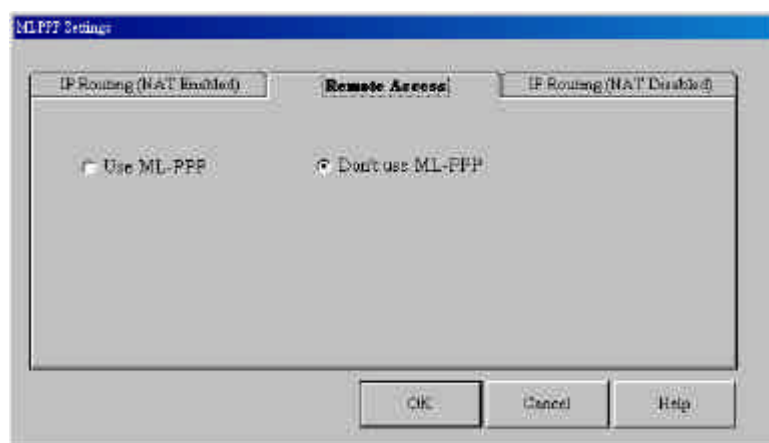
---

#### **Use ML-PPP**

Allow remote client to dial-in using ML-PPP protocol.

#### **Don't use ML-PPP**

Don't allow remote client to dial-in using ML-PPP protocol.



*LAN DHCP Server*

**DHCP Function**

By default the network device's DHCP server is enabled. If you would like to disable the DHCP server, click on the **Disabled** circle.

Click the **LAN DHCP Server** in the main screen to get the DHCP configuration screen displayed below.

What is a DHCP Server?  
Please see the DHCP entry in the Glossary at the back.

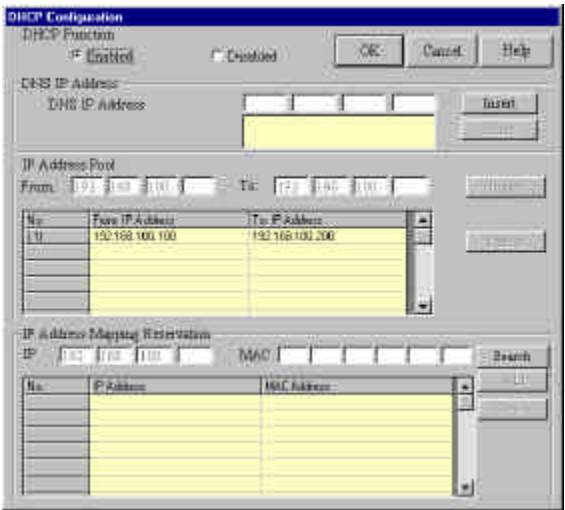


Figure 3.16 LAN DHCP Server screen

**DNS IP Address**

Enter the ISP's DNS IP address. You can insert a max of 4 ISP DNS's IP Addresses.

**IP Address Pool**

The IP Address Pool contains the range of the IP addresses that will automatically be assigned to the clients of your network. By default the IP address pool range is **From 100 To 200** (this/these range(s) will be listed in the **IP Address Pool** table). If you would like to change this range first select the range then enter a new range and press the **Insert** button.

To delete an IP address range select a range and then press the **Delete** button.

### IP Address Mapping Reservation

You can use the IP Address Mapping Reservation option to give a particular computers on your network the same static IP address every time the computer is turned on.

To assign a computer on your network a static IP address, you can enter the MAC address directly or you can use the MAC address search tool by entering the IP address of the computer and then using the **Search** button to find the MAC address. Press the **Add** button to reserve the IP address for this computer.

To delete a static IP address: Select it and then press the **Delete** button.

## Routing Settings

This function allows your network device to route IP packets to another network.

Click the Routing Settings in the main screen to get the Routing Settings screen displayed below.

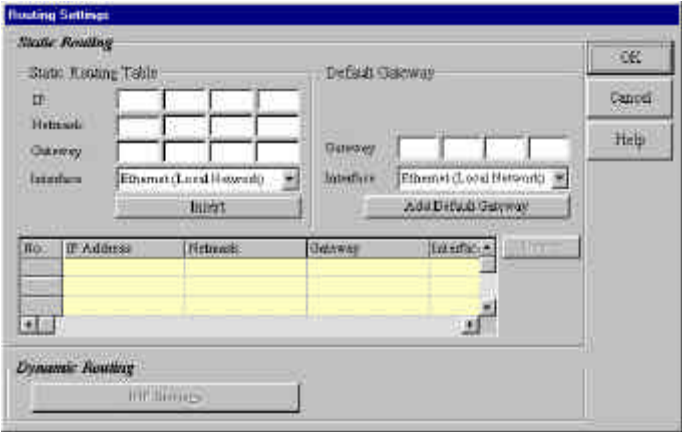


Figure 3.17 Routing Settings

### Static Routing Table

**IP** : The (Network/Subnet) IP address you want to route to.

**Netmask** : The subnet mask of the Network IP address.

**Gateway** : The IP address on your network that's linked to the other network/subnet.

**Interface** : Select which port (LAN or WAN etc.) interface the gateway is at..

Click **Insert** to save the information into the routing table. To Delete this information select it from the routing table and click **Delete**.

### Default Gateway

Default gateway is an IP address that all packets are routed to, when the device can't find a route match (the destination IP address of the packet in the routing table).

Click **Add Default Gateway** to save the IP address of the default gateway

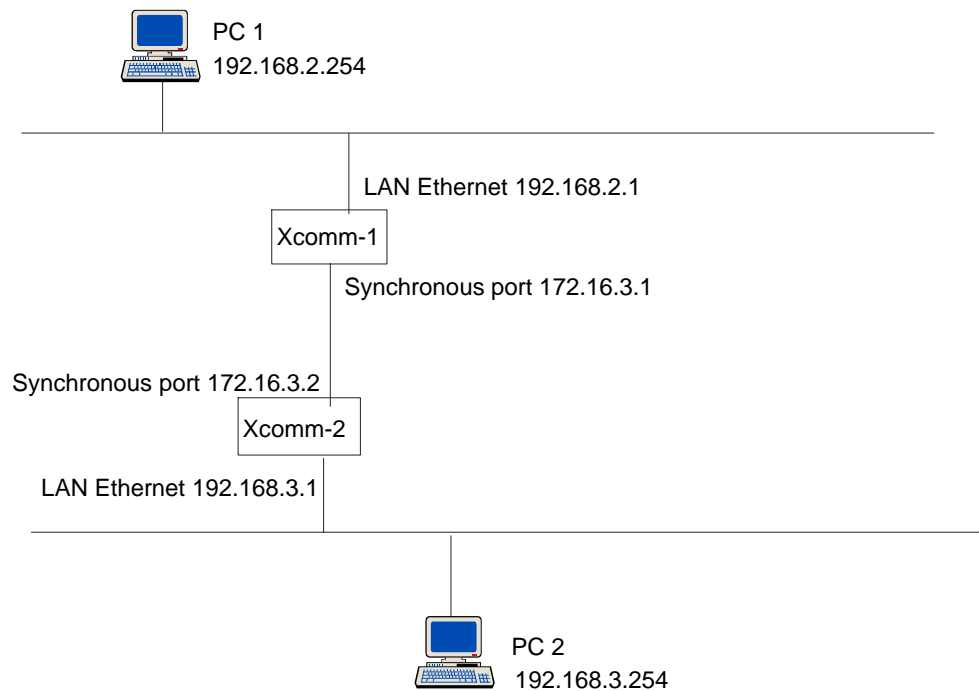
**Interface** : Select which port (LAN or WAN etc.) interface the gateway is at..

### 3 - Routing Settings

---

#### Routing Table

The routing table stores the routing information so that your network device know how to route the IP packets to the proper network.



#### What is the purpose of the routing table?

In the example, Xcomm-1 needs routing information to route between 192.168.2.x and 192.168.3.x. Therefore, if you want Xcomm-1 to route to the 192.168.3.x network, you would input the following routing table entry into the Xcomm-1 Routing Settings.

IP : 192.168.3.0  
Netmask : 255.255.255.0  
Gateway IP : 172.16.3.2  
Interface : Synchronous Port

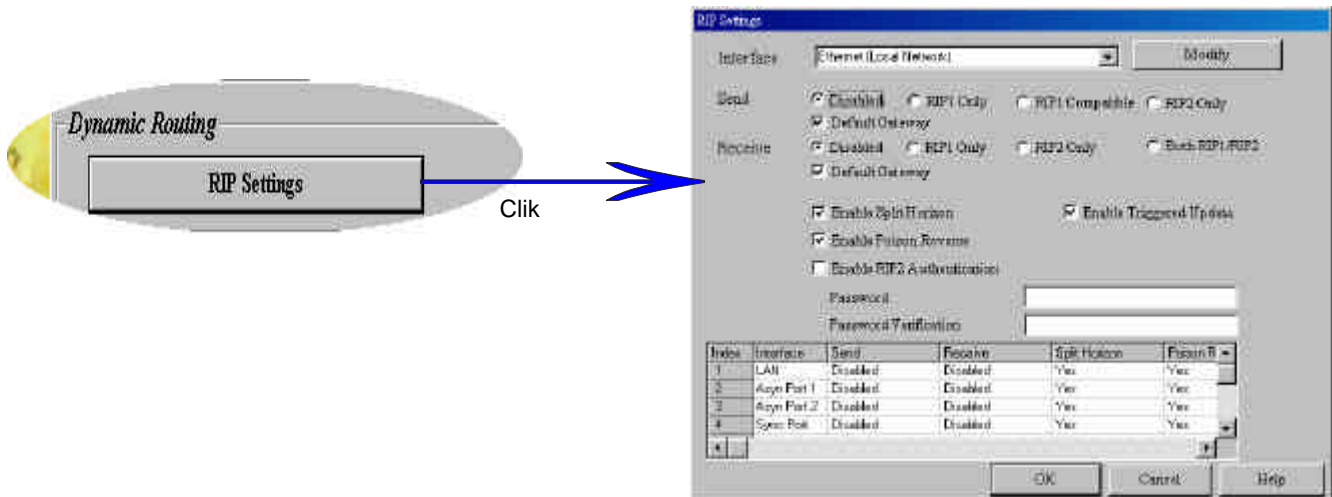
And if you want Xcomm-2 to route to 192.168.2.x, you would input the following routing table entry into the Xcomm-2 Routing Settings.

IP : 192.168.2.0  
Netmask : 255.255.255.0  
Gateway IP : 172.16.3.1  
Interface : Synchronous Port

## Dynamic Routing

### RIP Setting

Xcomm implements the most commonly used routing protocol RIP1/2 to support dynamic learning of routing.



### Interface

Specify the interface for RIP1/2 routing protocol. You can choose ethernet, synchronous port, asynchronous port1 or asynchronous port2.

### Send Method

#### Disabled -

You can specify to disable sending of the routing protocol.

#### RIP1 Only -

You can specify to send the RIP1 protocol only.

#### RIP1 Compatible -

You can specify to send RIP2 protocol using broadcast.

#### RIP2 Only -

You can specify to send RIP2 protocol only.

**If Default gateway is enabled, the router will send the default gateway message, through the interface.**

**Receive Method****Disabled -**

You can specify to disable to receive routing protocols from the interface.

**RIP1 Only -**

You can specify to receive RIP1 protocols from the interface only.

**RIP1 Compatible -**

You can specify to receive both RIP1 and RIP2.

**RIP2 Only -**

You can specify to receive the RIP2 protocol only.

**If Default gateway is enabled, the router will receive the default gateway message through the interface.**

**Enable Split Horizon**

Enable Split Horizon will never include routing information acquired from that interface when sending the RIP update over the particular interface.

**Enable Triggered Updates**

Enable Triggered Updates will send an update message to all its neighbors immediately without waiting for the usual periodic update cycle.

**Enable Poison Reverse**

Enable Poison Reverse will set the metric to infinity for those routes acquired over that interface.

**Enable RIP2 Authentication**

Enable RIP2 Authentication will include the password when sending RIP2 updates.

## Filter Settings

You can use the Filter Settings to choose which packets come into the LAN and/or which ones go out into the WAN port.

The filter settings allows you to filter which packets are allowed to either Pass (fig 13.18.2) or to be Blocked (fig 13.18.1)

Click the Routing Settings in the main screen (figure 3.1) to get the Routing Settings screen displayed below.

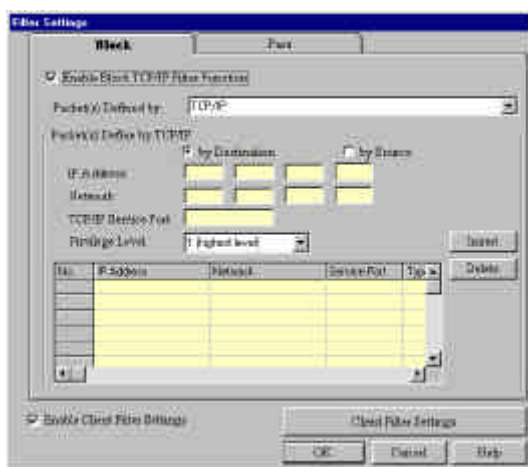


Figure 3.18.1 Block screen

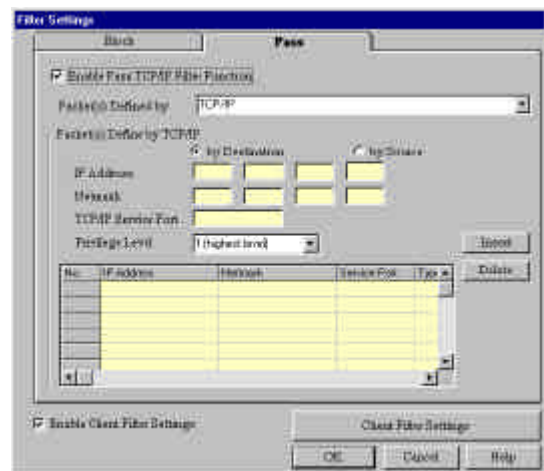


Figure 13.18.2 Pass Screen

**Block:** The settings in the Block screen allows you to define which packets are to be blocked from going out into the WAN port or coming into your LAN

**Pass:** The settings in the Pass screen allows you to define which packets can go out into the WAN port or come into your LAN

#### Enable Block TCP/IP Filter Function

Check this if you would like to define the Block Filter function

#### Enable Pass TCP/IP Filter Function

Check this if you would like to define the Pass Filter function

#### Packet(s) Defined by:

In order to filter packets, you have to define the packets that will be filtered. You have 2 choices, either to define the packet(s) by **TCP/IP** or by the **User**

- 1) **TCP/IP**
- 2) **User**

### 3 - Filter Settings

---

#### 1) Packet(s) Defined by **TCP/IP**

If you choose to define by TCP/IP you have to enter the IP information of the packet(s) and indicate whether it is the Destination or Source IP information by clicking **by Destination** or **by Source**.

**IP Address:** Input the IP address of the packet to be Block(ed) or allowed to Pass  
Note: Keep in mind whether you've checked **by Destination** or **by Source**.

**Netmask:** Input the subnet mask for the packet

**TCP/IP Service Port:** Input the Socket Port you would like to Block or allowed to Pass. (E.g. HTTP = 80)

#### **Privilege Level**

It is quite common for you to set many filter rules for a particular client. Some times the rules that you set for that client may conflict with each other. When there is a conflict for a particular client the Net Device will perform the filter rule with the higher privilege level (Level one (highest), Level sixteen (lowest) privilege level)

For example:

If you configure the following rule for **Source** IP address 192.168.100.72 with a privilege level of 16 to Pass using socket number 80 (see figure 3.19.1).

No.	Netmask	Service Port	Type	Privilege
1	168	80	TCP	16

Figure 3.19.1 Pass

No.	Netmask	Service Port	Type	Privilege
1	168	80	TCP	1

Figure 3.19.2 Block

And at the same time if you have the same filter rule that blocked IP address 192.168.100.72 with a privilege level of one (see figure 3.19.2).

Then the Net Device will block the IP address 192.168.100.72, because it has a higher privilege level.

**Note:** If conflicting rules have the same privilege level then the Net Device will Block the packet.

Click **Insert** when you've defined all of the above information. To delete a defined packet, select the packet in the table and click **Delete**.

### 2) Packet(s) Defined by **User**

If you choose to define by User you will have to define the byte pattern of the packet(s). The Network Device will use the byte patterns that you defined in the screens below to block or allowed to pass from the WAN or from the LAN.

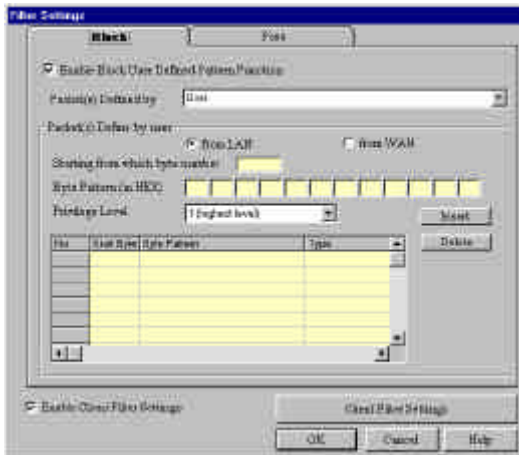


Figure 3.20.1 User Block screen

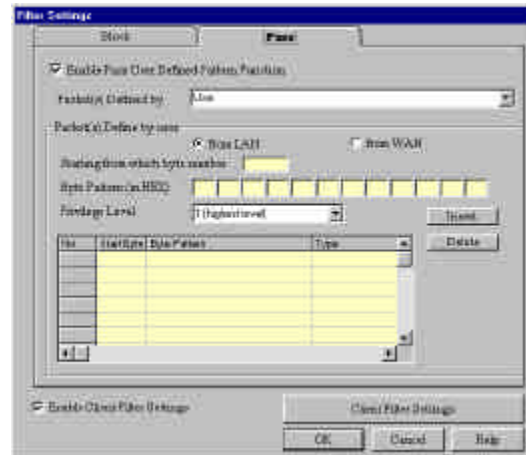


Figure 3.20.2 User Pass screen

**Block** The settings in the Block screen allows you to define which packets are to be blocked from going out into the WAN port or coming into your LAN

**Pass** The settings in the Pass screen allows you to define which packets can go out into the WAN port or come into your LAN

#### Enable Block User Defined Pattern Function

Check this if you would like to define the Block Filter function

#### Enable Pass User Defined Pattern Function

Check this if you would like to define the Pass Filter function

#### Starting from which byte number

Here you can indicate which byte in the packet the net device should start to read the byte pattern that you've entered in the **Byte Pattern (in Hex)** in order to see if it's a packet that needs to be filtered.

#### Byte Pattern (in Hex)

Enter the packet byte patterns that you would like the net device to recognize as a packet to be filtered.(Block/ Pass from the WAN/ LAN)

Click **Insert** when you've defined all of the above information. To delete a defined packet, select the packet in the table and click **Delete**,

### 3 - Filter Settings

---



#### Enable Client Filter Settings

Check the *Enable Client Filter Settings* to enable the parameters that you defined in the *Client Filter Settings*

#### Client Filter Settings

The Client Filter lets you decide what services are allowed into your network and who is authorized to access them.

#### Privileged Clients (fig 3-23)

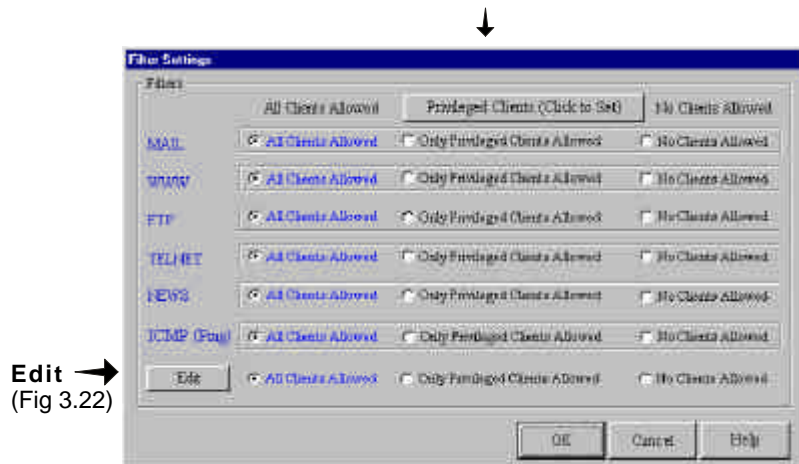


Figure 3.21 Client Filter Settings

The filter works by filtering TCP/IP port numbers. There are 5 main port numbers that we have listed corresponding to 5 different services (Mail, WWW, FTP, Telnet, News). If you would like to filter other services that are not listed; then you must know the port number of that service. These port numbers can then be entered in **Edit** of the filter setting screen.

Edit(Customize filter)

- 1) enter Port # here
- 2) Click Add

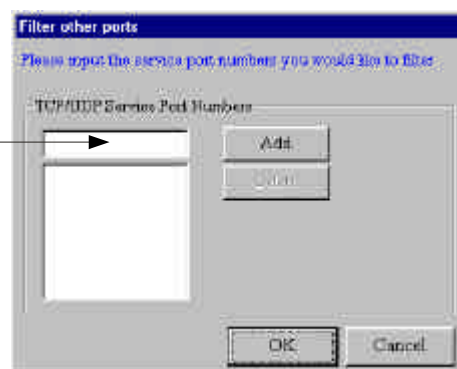


Figure 3.22 Edit Filtered Port Settings.

What is a Port ?

Please see the Port entry in the Glossary at the back.

**Privileged Clients**

Click Privileged clients in the Filter Settings screen to display the screen below

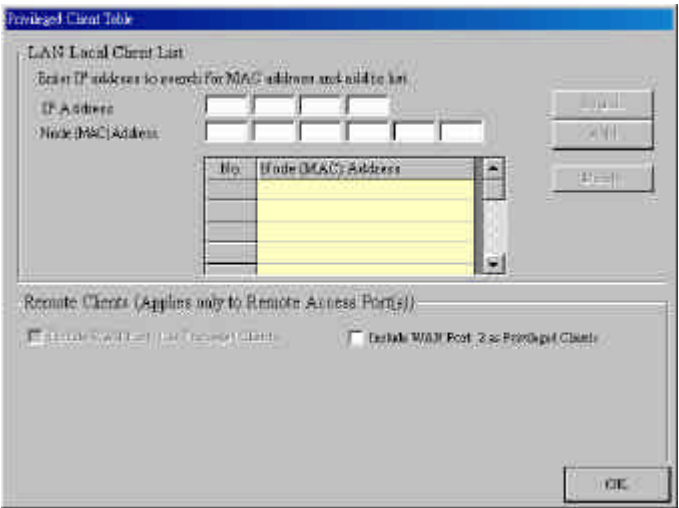


Figure 3.23 Privileged Clients Settings

**LAN Local Client List**

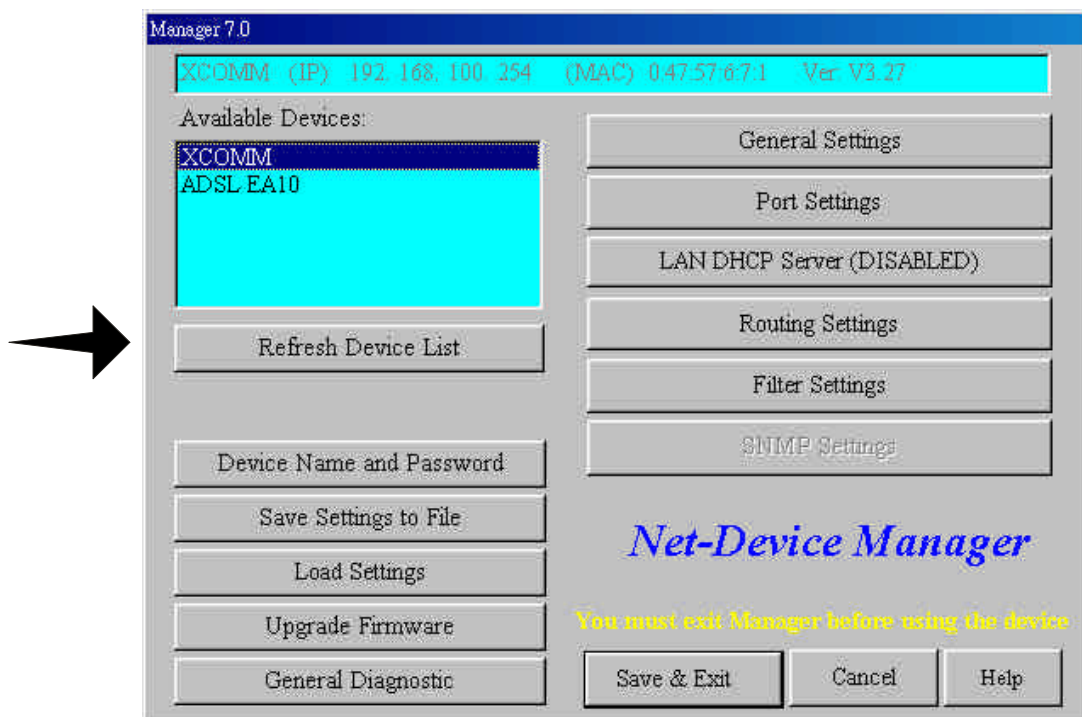
In the privileged client's table enter the clients that you wish to have privileged access to the services that you have selected in the Filter Settings screen. The Client filter uses MAC addresses to identify the privileged clients. You can enter the MAC address directly or you can use the MAC address search tool by entering the IP address of the computer and then using the Search button to find the MAC address. Once you have filled out the IP Address and Node (MAC) Addresss , click Add to add the information to the Node (MAC) Address list.

**Remote Clients (Applies only to Remote Access Port(s))**

You can also filter Remote Clients by the WAN ports that they are coming in from by checking the ☒ **Include WAN Port 2 as Privileged Clients.**

#### *Refresh Device List*

By clicking the Refresh Device List button in the Net Manager's main screen below the Network Manager will search for available Network Devices on your LAN and will display them in the **Available Devices** section.



What if the device is not found displayed?

Click the **Refresh Device list** and see if the Network Device shows up, if not, please make sure that all cables are correctly plugged-in, connected and that the device is powered on.

#### Device Name and Password

You can give your device a name and a password in this section.

Click the Device Name and Password in the main screen (figure 3-1) to get the Device Name and Password screen displayed below.

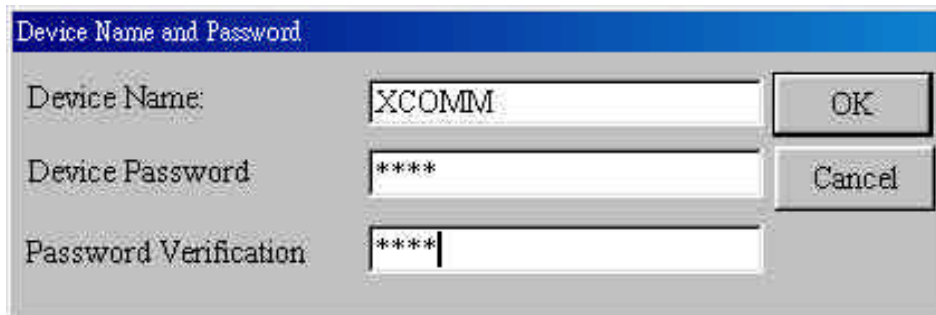


Figure 3.24 Device Name and Password Screen

#### Device Name

This field displays the name of your network device. If you would like to change this name, enter the new name in this field.

If you are connecting a cable modem/ADSL to an ISP, the device name can act as your computer name, if your ISP requires you to input a computer name.

#### Device Password

The Net-Device Manager does not come with a password. If you choose to give your network device a password, this password will be required the next time and subsequent times that you want to configure your network device. To enter a password, type your password in the Device Password field and type it again in the Password Verification field.

If you choose to enter a password pick something that is easy to remember and write it down in a safe location. If you have completely forgotten your password please contact your place of purchase.

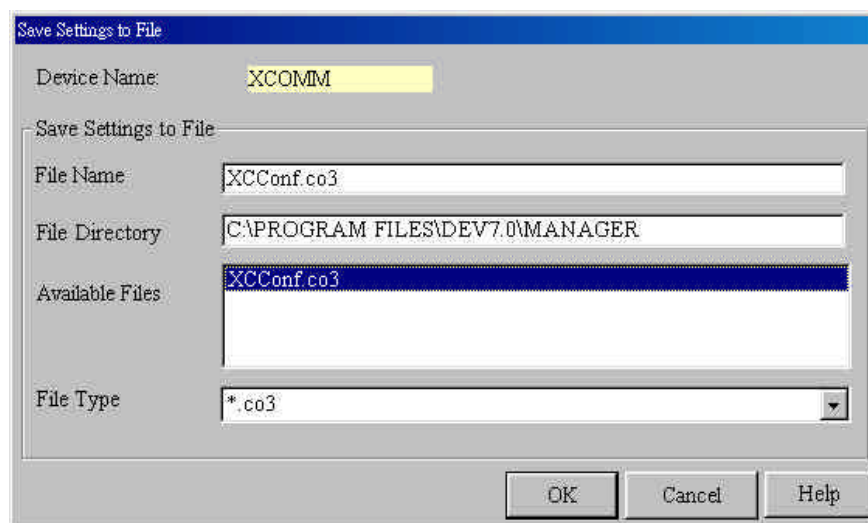
### 3 - Save Settings to File

---

#### Save Settings to File

The Save Settings to File option lets you save the inputted settings to a file to be retrieved at a later time. This will be useful if your settings are deleted accidentally or you want to have more than one batch of settings.

Click the **Save Settings to File** in the main screen (figure 3-1) to get the Save settings to File screen displayed below.



The screenshot shows a Windows-style dialog box titled "Save Settings to File". It has a light gray background and a blue title bar. The dialog contains several input fields and a list box. The "Device Name" field is labeled "Device Name:" and contains the text "XCOMM". Below it is a section titled "Save Settings to File" which contains four sub-fields: "File Name" with the text "XCConf.co3", "File Directory" with the text "C:\PROGRAM FILES\DEV7.0\MANAGER", "Available Files" with a list box containing "XCConf.co3", and "File Type" with a dropdown menu showing "\*.co3". At the bottom right of the dialog are three buttons: "OK", "Cancel", and "Help".

Figure 3.25 Save Settings to File Screen

To save the inputted settings to a file.

- 1) Enter the file name in the File Name field

Please leave the file type extension as its default entry because if you try to use the **Load settings** unction the manager program will look for the specific file extension that is compatible with your device.

XCOMM File Type will be \*.co3

- 2) Press the **OK** button to save the settings to a file.

### *Load Settings*

The Load Settings option lets you load the original default settings of your network device or a previously saved settings.

Click the **Load Settings** in the main screen (figure 3-1) to get the Load Settings screen displayed below.

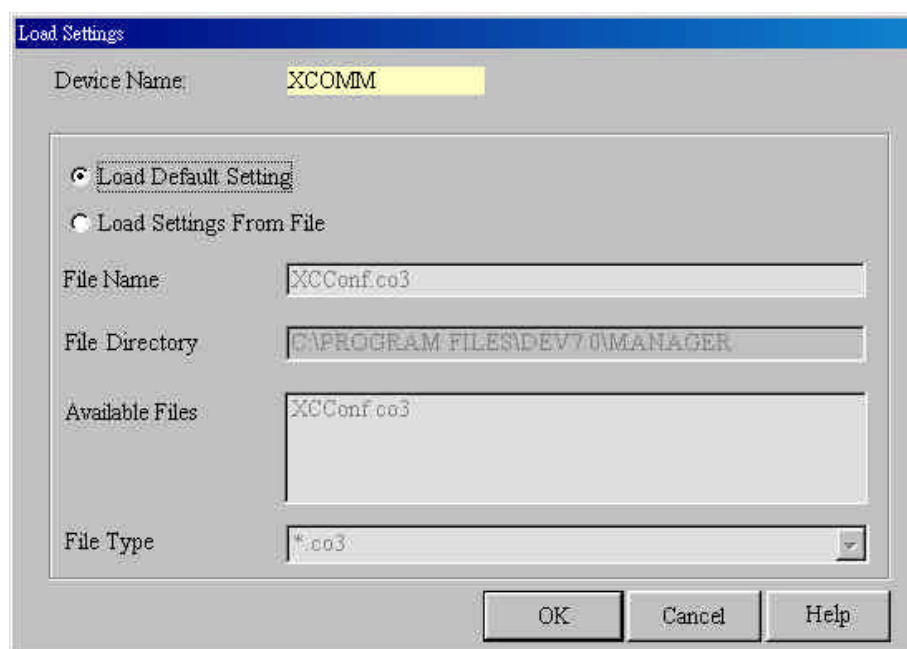


Figure 3.26 Load Setting Screen

First choose whether you want to load the default settings or load settings from a previously saved file. If you want to load the **default Setting** :

- 1) Check Load Default Setting.
- 2) Click the **OK** Button.

If you are loading previously saved settings from a file (**Load Settings from file**) :

- 1) Choose the directory by entering it in the **File Directory** field and then select the file from the **Available Files** table.
- 2) Press the OK button to load and apply the previous settings to your network device.

### *Upgrade Firmware*

The Upgrade Firmware option allows you to upgrade the firmware that is in your Network Device.

Click the **Upgrade Firmware** in the main screen (figure 3-1) to get the Upgrade Firmware screen displayed below.

What is a Firmware ?

Please see the Firmware entry in the Glossary at the back.

This function upgrades the firmware actually in your network device and not the Net-Device Utilities.

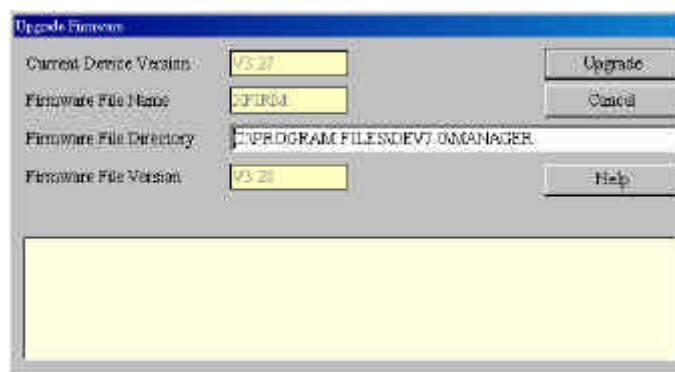


Figure 3.27 Upgrade Firmware Screen

How to upgrade a Firmware :

1) Enter the location of the new firmware file in the **Firmware File Directory**. Net-Device Manager will automatically detect the new firmware name and will display it in the **Firmware File Name** field. The **Firmware File Version** will display the version number of your new firmware.

2) Click **Upgrade** to upgrade the new Firmware.

Note : Normally the procedures to upgrade the firmware are :

1. Get the newest firmware from distributors or at our web site  
[Http://www.arguscorp.com/support/index.htm#C](http://www.arguscorp.com/support/index.htm#C)
2. Copy the firmware to the directory of the P C. (Eg. C:\progra~1\Dev7.0\Manager)
3. The firmware version will be displayed in the Firmware File Version field automatically.
4. Click Upgrade.

Warning!

Upgrade is a dangerous process that might corrupt the execution of the device.  
Without distributor's permission, upgrade is not recommended.

## *General Diagnostic*

General Diagnostic displays your network device's information.

The general diagnostic function will perform a check-up on your network device to make sure that everything is functioning correctly.

To open the general Diagnostic click the General Diagnostic button in the main menu (fig 3-1)

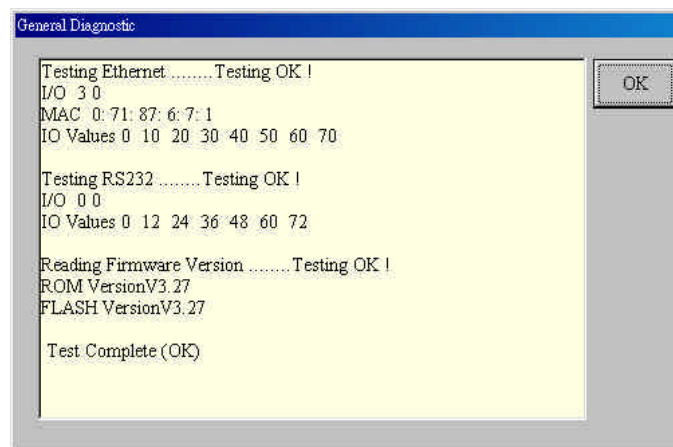


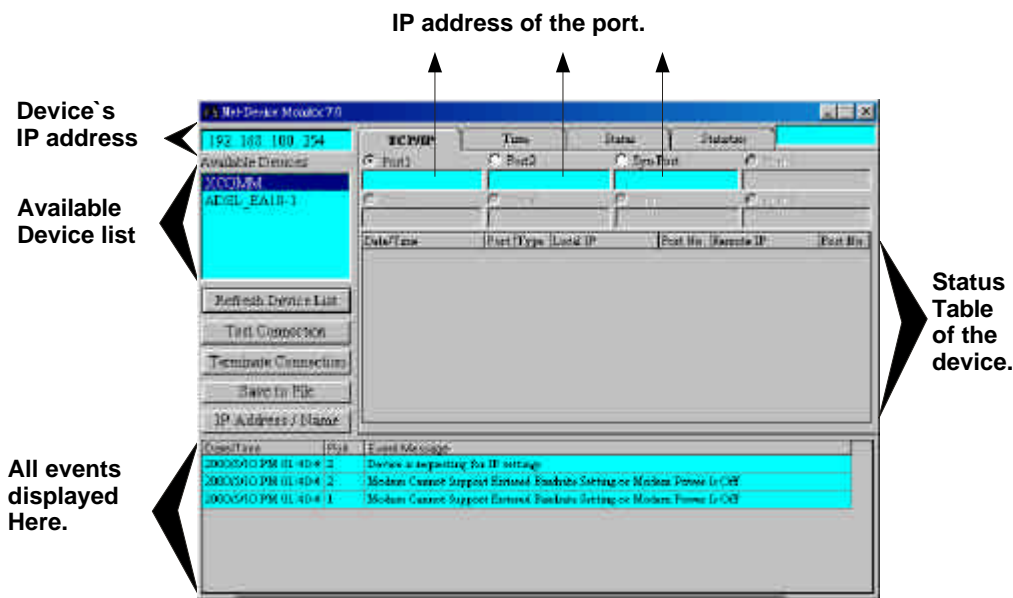
Figure 3.28 General Diagnostic screen

**Net-Device Monitor**

Net-Device Monitor is a utility that was designed for letting you know what your Network Device is doing and helping you solve problems.

**To Run Net-Device Monitor from your Desktop**

On the Windows/95/98/NT/2000 `Start` menu point to `program`, then to `Net-Device` and select `Monitor`.



The name of the device will be shown on the **Available Device** list. In the example above, 2 devices ,XCOMM and ADSL\_EA10 are in the local network.

If `device is not found` is shown, see **Trouble Shooting**.

### Refresh Device List

By clicking the Refresh Device List button in the Net Manager main screen below the Network Manager will search for available Network Devices on your LAN and will display them in the **Available Devices** section.

### Test Connection

This will test if you have inputted some of the major settings in the Network Device correctly and whether a problem you may have is due to the modem, Network Device or some other setting that you may have inputted incorrectly.

To test a connection, just click on the **Test connection** button.

Test connection will then use the asynchronous port and the modem attached to it to dial-up to the remote server (ISP) and establish a connection.

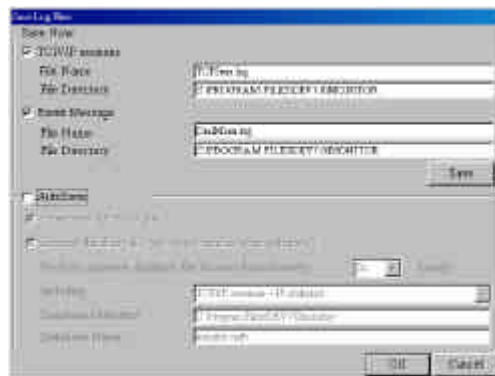
### Terminate Connection

The Terminate Connection function was designed to allow the network administrator the ability to terminate the Network Device's connection instantly at any time.

To terminate a connection of a particular Network Device select the server in the **Available Devices** box, and press **Terminate Connection**

### Save to File

If you would like to save a monitoring sessions to a file you can click the **Save to File** Button.



### Save Now

If you wish to save the monitor display now, first select which monitor displays you wish to save(TCP/IP, Event Message). You can choose the file name and file directory that you would like to save the files to Press the Save button to save to the file.

### Autosave

If you wish to periodically save the monitor display to a database file, enable the autosave function. Options include:

1) Overwrite database file

Will periodically save the monitor display to a database file based on the time that you specify, Overwriting the last saved database file.

2) Append database file (will reset after autosave)

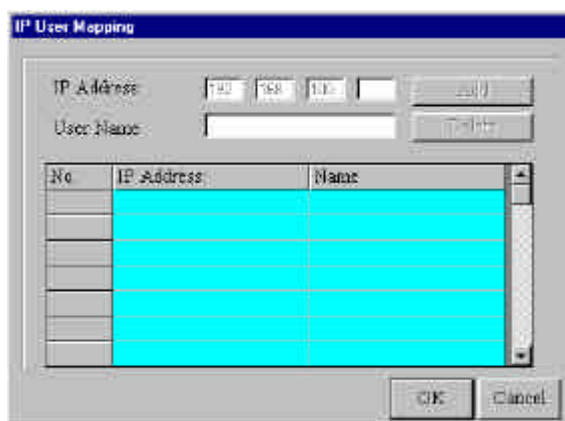
Will automatically save the monitor display to a database file based on the time that you specify, updating and Appending to the file. Please note that with this option after autosave has appended the date to the database, the monitor will reset and the display screens will be cleared.

## 4 - Net-Device Monitor

---

### IP Address / Name

This function will let you associate a name with a specific IP address and name on your computer and will be displayed in the relevant monitor displays. This will make it easier for you to see which users are transmitting or receiving data without having to remember their specific IP addresses. For this function to work you must give these users fixed IP addresses on your network. This can be done on each individual computer or by using your network device's DHCP server IP reservation system.



### Event Messages

The event message display located in the lower part of Net-Device Monitor, displays the communication occurring between your network device, modem/ISDN TA and remote server (ISP)..

Date/Time	Port	Event Message
4/17/00 5:06:42 PM	2	Modem is Ready DTE Speed 115200 bps
4/17/00 5:06:49 PM	1	Test Connection initiated
4/17/00 5:08:30 PM	2	Incoming Call for Remote Access
4/17/00 5:08:34 PM	2	Modem is Connected
4/17/00 5:08:34 PM	2	Start PPP
4/17/00 5:08:36 PM	2	PPP is Connected (IP protocol is Ready to Send/Receive)
4/17/00 5:08:42 PM	2	Line Disconnected (by Remote Site)

You can use your mouse to point and click on any of the event messages to bring up a help screen. If any errors occur you can use this as a guide to help you fix the problem.

### TCP/IP Tab

The TCP/IP Tab displays all the TCP/IP requests made by your Network Device. You can select to view TCP/IP sessions in the **Sync Port** or the **Async port**.

Note: The TCP/IP sessions displayed on the screen is useful to record the history of the TCP/IP session through the selected port. But, the TCP/IP sessions displayed does not indicate the connection status of the sessions.

**Date/Time** : Tells you when the request was made

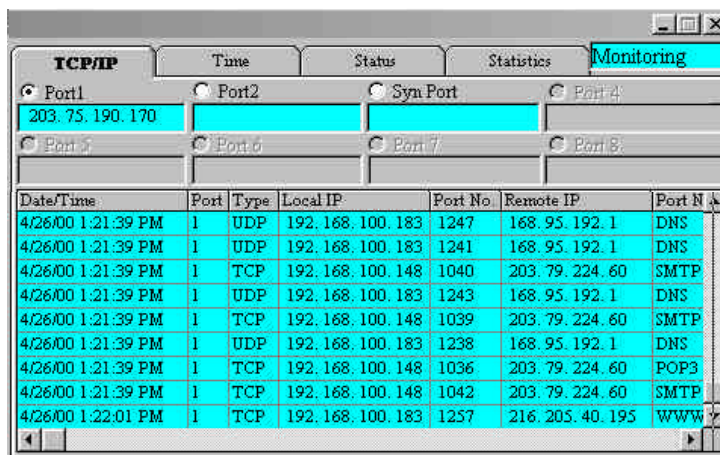
**Port** : Tells you which port you are viewing

**Type** : Tells you what type of request is being made

**Local IP** : Tells you which IP address the request originated from.

**Remote IP** : Tells you which IP address was requested.

**Port Number** : Tells you which TCP/IP port was requested.



The screenshot shows a window titled 'TCP/IP' with tabs for 'Time', 'Status', 'Statistics', and 'Monitoring'. The 'Monitoring' tab is active. Below the tabs are radio buttons for 'Port1', 'Port2', 'Syn Port', and 'Port4'. 'Port1' is selected, and the IP address '203.75.190.170' is entered. Below these are more radio buttons for 'Port5', 'Port6', 'Port7', and 'Port8'. A table displays the following data:

Date/Time	Port	Type	Local IP	Port No.	Remote IP	Port No.
4/26/00 1:21:39 PM	1	UDP	192.168.100.183	1247	168.95.192.1	DNS
4/26/00 1:21:39 PM	1	UDP	192.168.100.183	1241	168.95.192.1	DNS
4/26/00 1:21:39 PM	1	TCP	192.168.100.148	1040	203.79.224.60	SMTP
4/26/00 1:21:39 PM	1	UDP	192.168.100.183	1243	168.95.192.1	DNS
4/26/00 1:21:39 PM	1	TCP	192.168.100.148	1039	203.79.224.60	SMTP
4/26/00 1:21:39 PM	1	UDP	192.168.100.183	1238	168.95.192.1	DNS
4/26/00 1:21:39 PM	1	TCP	192.168.100.148	1036	203.79.224.60	POP3
4/26/00 1:21:39 PM	1	TCP	192.168.100.148	1042	203.79.224.60	SMTP
4/26/00 1:22:01 PM	1	TCP	192.168.100.183	1257	216.205.40.195	WWW

What is a Port?

Please see the 'Port' entry in the glossary at the back.

### Connection Time Tab

**Device power turned on**

Displays the time/date of your Network Device when it was turned on.

**Power-On-Time**

displays the total time that has elapsed since your Network Device was turned on.

**Total Connection Time**

displays the total connection time for each port that has been logged on since the device was turned on.

**Current Connect**

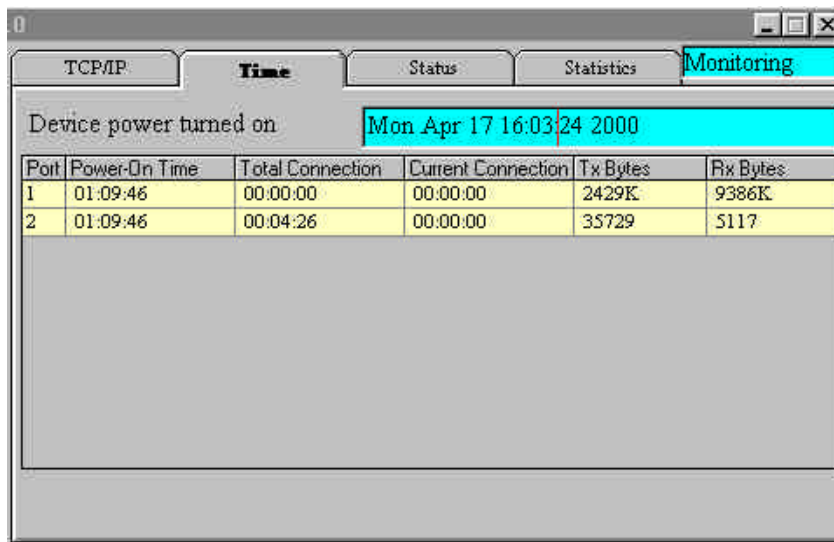
displays the time that has elapsed since the current connection was established for the port.

**TX Bytes**

displays the total amount of bytes transmitted since your Network Device was last turned on for each port.

**RX Bytes**

displays the total amount of bytes received since your Network Device was last turned



The screenshot shows a window titled '0' with a tabbed interface. The 'Time' tab is selected, showing 'Device power turned on' as 'Mon Apr 17 16:03:24 2000'. Below this is a table with 6 columns: Port, Power-On Time, Total Connection, Current Connection, Tx Bytes, and Rx Bytes. Two rows of data are visible for ports 1 and 2.

Port	Power-On Time	Total Connection	Current Connection	Tx Bytes	Rx Bytes
1	01:09:46	00:00:00	00:00:00	2429K	9386K
2	01:09:46	00:04:26	00:00:00	35729	5117

### Status Tab

#### Async Port (Port 1 and Port 2), Synchronous Port3

**Modem Power:**

If the Network Device detects that your modem is turned on, this indicator light will be lit.

**Modem Ready:**

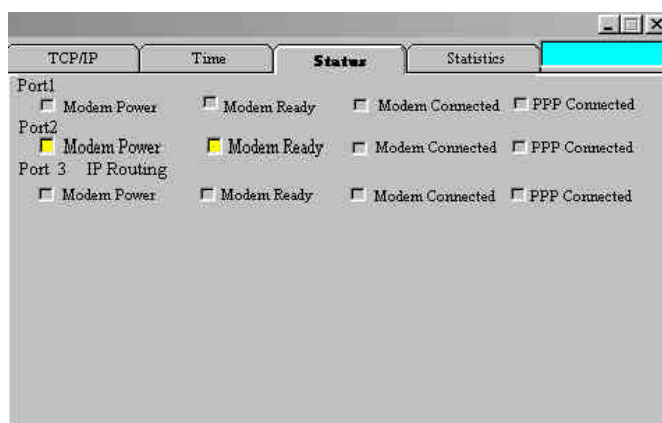
The Network Device will send pre-initial and initial commands to your modem or ISDN TA. If the communication is successful, this indicator light will be lit and your modem is ready to dial a connection.

**Modem Connected:**

If the Network Device has detected that your modem has successfully dialed up a connection to a remote site, this indicator light will be lit.

**PPP Connected:**

After the connection is established, if the Network Device has detected that PPP has successfully connected, this indicator light will be lit.



### Statistics Tab

The statistics tab will let you know how many bytes of data has come in and out through your network device and through which ports. The statistics tab will display each IP address's **TX Bytes**, **RxBytes** and **Total Bytes** information:

#### **Tx Bytes:**


the number of bytes transmitted from the computer with this IP address.

#### **Rx Bytes:**

the number of bytes received from the computer with this IP address.

#### **Total Bytes:**

the total number of bytes that has been received and transmitted from the computer with this IP address.



The screenshot shows a window titled "Net-Device Monitor" with four tabs: "TCP/IP", "Time", "Status", and "Statistics". The "Statistics" tab is selected and highlighted in blue. Below the tabs is a table with four columns: "IP Address:", "Tx Bytes", "Rx Bytes", and "Total Bytes". The table contains eight rows of data. A "Reset" button is located at the bottom right of the window.

IP Address:	Tx Bytes	Rx Bytes	Total Bytes
192.168.100.51	740	1018	1758
192.168.100.66	9676	79K	89K
192.168.100.100	12519	845K	857K
192.168.100.105	1863K	5016K	6879K
192.168.100.140	5497	6428	11925
192.168.100.181	45	464	509
192.168.100.190	45195	1683K	1727K
192.168.100.223	498K	1551K	2049K

## Remote Access Settings

### Overview

There are separate configurations for Windows 95/98 that you must set to dial-in to the device to access Windows NT, Novell and Unix. This Section will go through all the settings needed for your Windows 95/98 to connect to these different servers.

Setting up a Remote Windows 95/98 Client to access a Windows NT Server

Open your Windows 95/98 Network Windows

1. In the Windows 95/98 Start menu, point to Settings and click Control Panel.
2. Double click the Network icon to open the Network Properties Display.

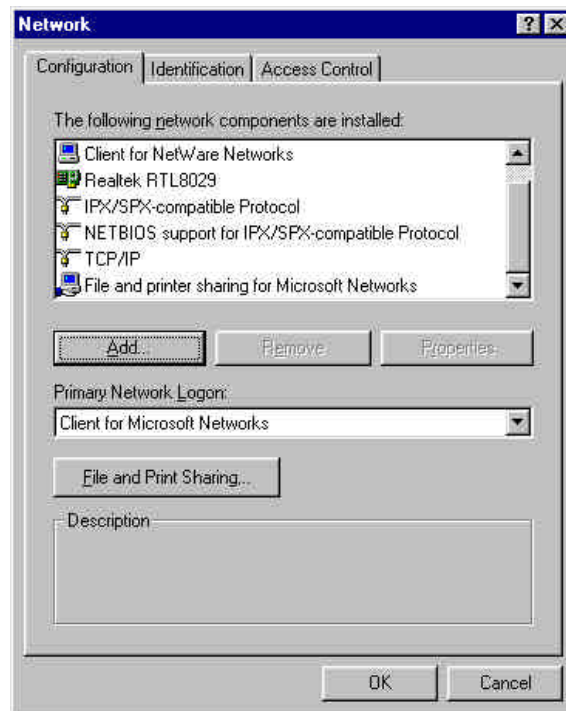
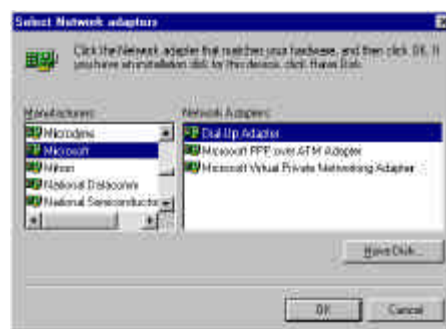
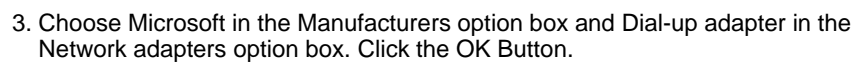


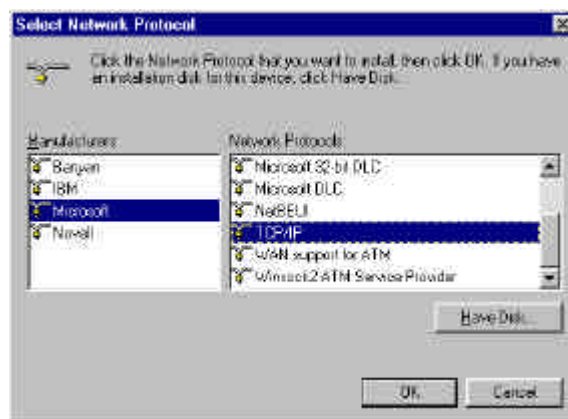
Figure 5-1

1. Click the Add button.
2. Select Adapter and click the add button.



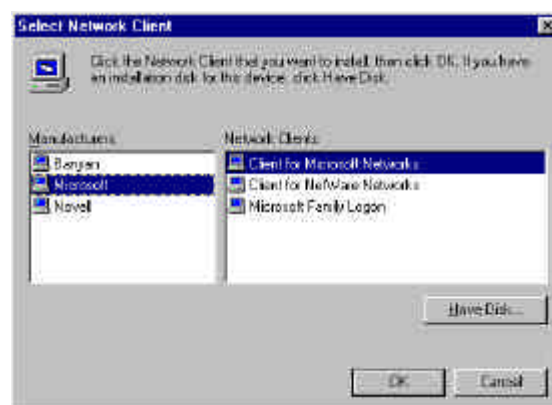
## Add TCP/IP Protocol

1. Click the Add button
2. Select Protocol and click the Add button.
3. Choose Microsoft in the Manufacturers option box and TCP/IP in the Network Protocols option box.
4. Click the OK button.



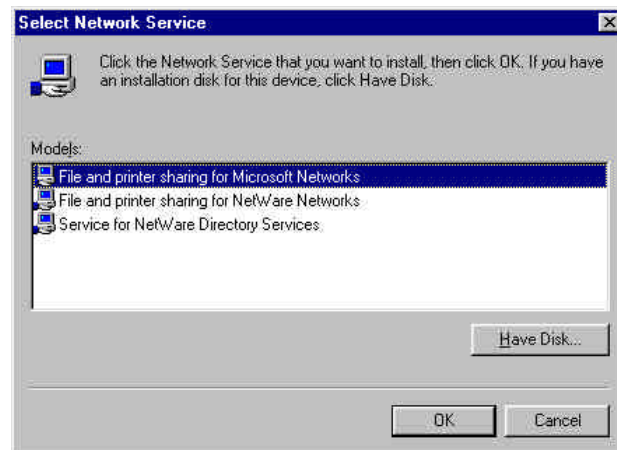
## Add Client for Microsoft Networks

1. Click the Add button
2. Select Network Client and click the Add button.
3. Choose Microsoft in the Manufacturers option box and Client for Microsoft Networks in the Network Clients option box.
4. Click the OK button.



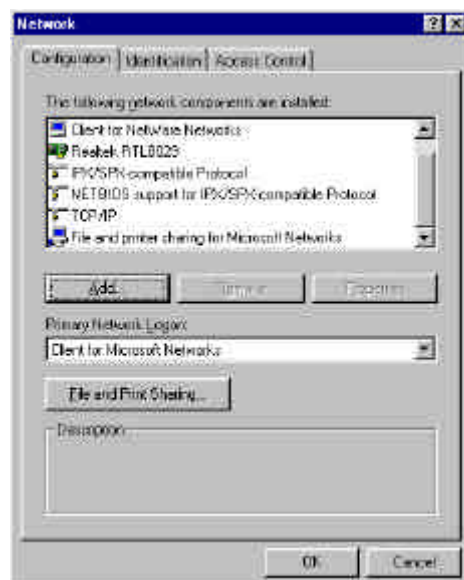
## Add File & Print Sharing for MS Networks

1. Click the Add button
2. Select Services and click the Add button.
3. Choose Microsoft in the Manufacturers option box and File and Printer Sharing for Microsoft Networks



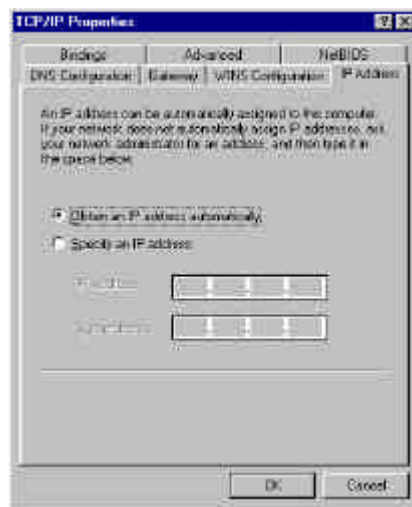
## Set Your Primary Network Logon

In the Primary Network Logon drop down menu, select Client for Microsoft Networks.



## Setup Properties of Components

1. In 'The following components are installed' window, select TCP/IP -> dial-up Adapter and click the Properties button to open the TCP/IP Properties Screen. On the IP Address tab make sure Obtain an IP address automatically is selected and press OK.



2. In 'The following components are installed' windows, select Client for Microsoft Networks and click the Properties button. On the General tab, enable the 'Log On to Windows NT Domain' check box. In the Windows NT Domain field enter the name of your windows NT Domain and press OK.



## Set your Identification

1. On the Network windows select the Identification tab.
2. In the Workgroup field enter the name of your NT domain. If you are not sure what the name of your NT domain is , please ask the administrator of your NT server.
3. Enter a name for your computer and a description of your computer in the Computer Name And Computer Description fields. There are for personal use only and can be anything you wish.



## Set Your Access Control

1. In the Network windows select the Access Control tab.
2. In the 'Control Access to shared resources using:' option box, select Shared-level access control



NOTE : Now you must restart your Windows 95/98 in order to have settings you just made to take effect.

### Make Your New Connection

1. Double Click the My Computer icon on your Desktop.
2. Open up your Dial-up Networking Folder.
3. Configure a new dial-up connection by double clicking the Add New Connection button.
4. Follow the instructions to completion.

### Set Dial-up Type

1. After you have made your new connection, select it, click the right mouse button and Select Properties.
2. Click the Server Type button and select PPP: Internet, Windows NT Server, Windows95/98.
3. Enable ONLY log on to Network, Enable Software Compression and TCP/IP as shown below.
4. Enable TCP/IP.

### Dial-up your network

You are now ready to dial-up your network device. Double click on the new connection that you have made and enter the user name and password that is configured for you in your network device. Press the Connect button. After you have connected to your network device, your remote Windows 95/98 computer will behave exactly like a real node on your network.

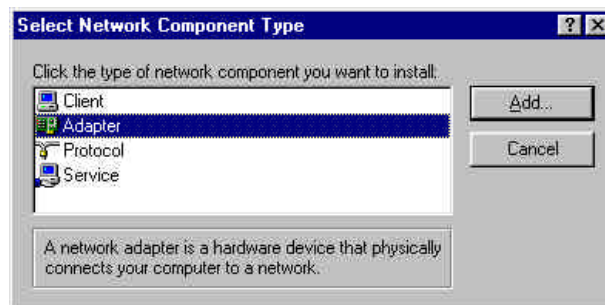
## Setting up a Remote Windows 95/98 Client to access a Novell Netware Server

### Open Your Windows 95/98 Client Network Windows

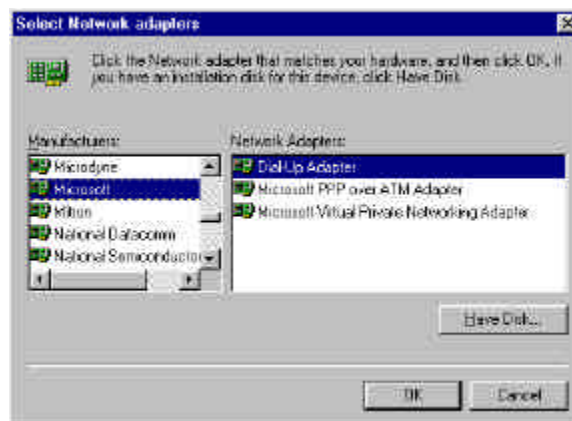
1. In the Windows 95/98 Start menu, point to Settings and click Control Panel.
2. Double click the Network icon to open the Network Properties Display.

### Add Microsoft Dial-up Adapter

1. Click the Add button
2. Select Adapter and click the add button.

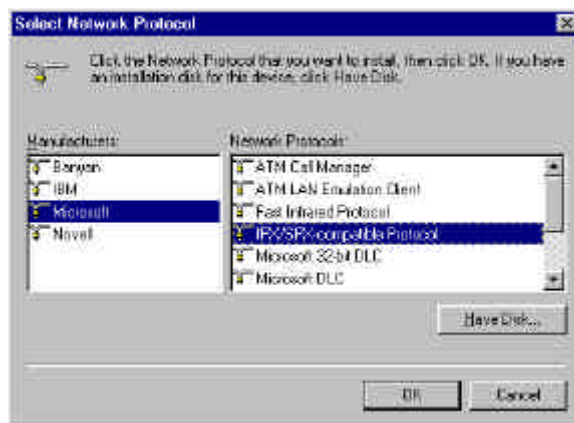


3. Choose Microsoft in the Manufacturers option box and Dial-up adapter in the Network Adapters option box. Click the Button OK.



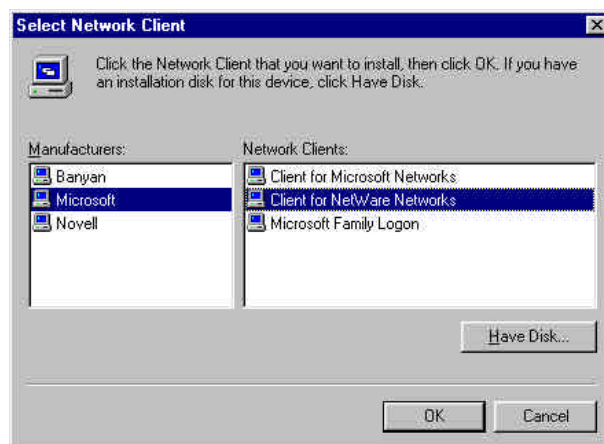
#### Add IPX/SPX Protocol

1. Click the Add button
2. Select Protocol and click the Add button.
3. Choose Microsoft in the Manufacturers option box and IPX/SPX Compatible Protocol in the Network Protocols option box.
4. Click the OK button.



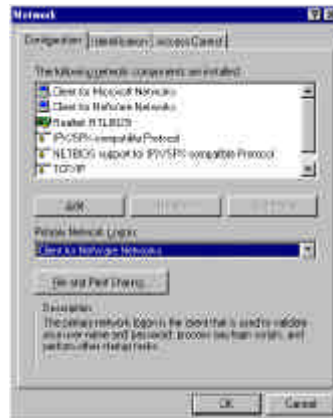
#### Add Client for Netware Networks

1. Click the Add button
2. Select Network Client and click the Add button.
3. Choose Microsoft in the Manufacturers option box and Client for Netware Networks in the Network Clients option box.
4. Click the OK button.



## Setup Properties of Components

In the Primary Network Logon drop down menu, select Client for Netware Networks.



## Set Your Primary Network Logon

In 'The following components are installed' windows Select Client for NetWare Networks and click the Properties button. On the General tab, in the 'Preferred Server' enter the name of your Novell Network Server Domain and select the and select First Network Drive and select Enable Logon Script processing.



### Set Your Access Control

1. In the Network Windows select the Access Control tab.
2. In the 'Control Access to shared resources using:' option box, select Shared Level Access Control.



#### NOTE:

You must restart your Windows 95/98 now in order to have settings that you just made to take effect.

### Make Your New Connection

1. Double Click the My Computer icon on your Desktop.
2. Open up your Dial-up Networking Folder.
3. Configure a new dial-up connection by double clicking the Add New Connection Button..
4. Follow the instructions to completion.

### Set Dial-up Type

1. After you have made your new connection, select it, click the right mouse button and Select Properties.
2. Click the Server Type button and select PPP : Internet, Windows NT Server, Windows 95/98.
3. Enable ONLY Log on to Network, Enable Software Compression and IPX/SPX as shown in the diagram.
4. Enable IPX/SPX compatible.

### Dial-up your network device

You are now ready to dial-up your network device. Double click on the new connection that you have made and enter the user name and password that is configured for you in your network device. Press the Connect button. After you have connected to your network device, your remote Windows 95/98 computer will behave exactly like a real node on your network.

Setting up a Remote Windows 95/98 Client to Access a Windows NT Server and Novell NetWare Server.

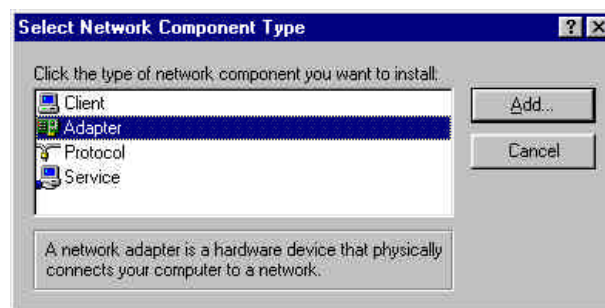
Note:: Before going to your remote site to configure the client please first make sure that the Windows NT Server has TCP/IP already installed.

Open Your Windows 95/98 Client Network Windows

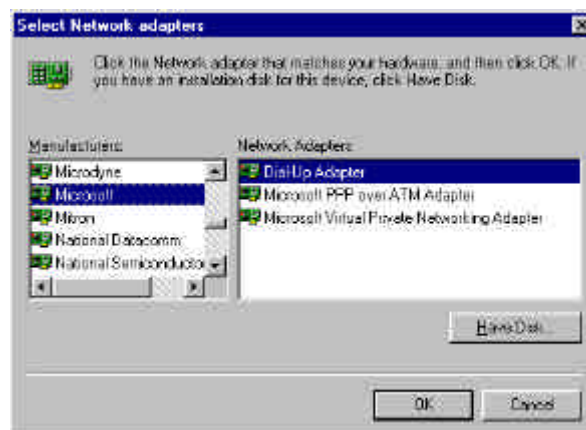
1. In the Windows 95/98 Start menu, point to Settings and click Control Panel.
2. Double click the Network icon to open the Network Properties Display.

Add Microsoft Dial-up Adapter:

1. Click the Add button
2. Select Adapter and click the add button.

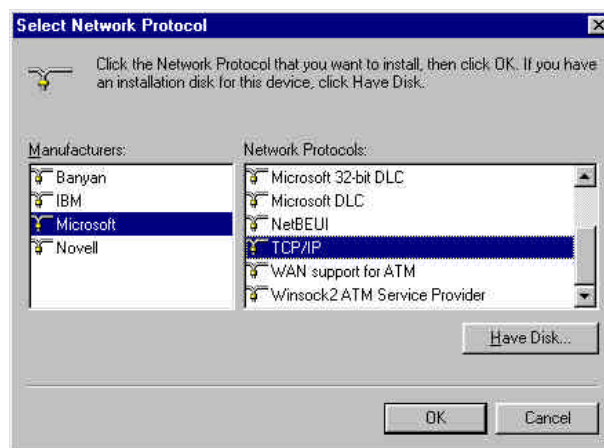


3. Choose Microsoft in the Manufacturers option box and Dial-up adapter in the network adapters option box. Click the OK Button.



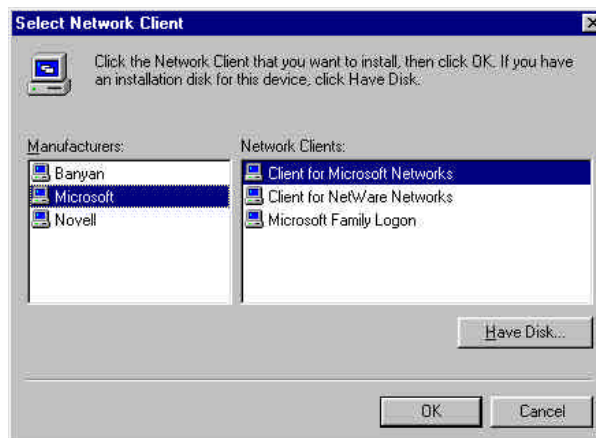
## Add TCP/IP Protocol

1. Click the Add button
2. Select Protocol and click the Add button.
3. Choose Microsoft in the Manufacturers option box and TCP/IP in the Network Protocols option box.
4. Click the OK Button.



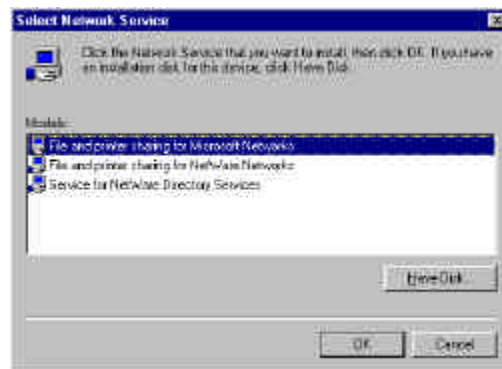
## Add Client for Microsoft Networks

1. Click the Add button
2. Select Network Clients and click the Add button.
3. Choose Microsoft in the Manufacturers option box and Client for Microsoft Networks in the Network Clients option box.
4. Click the OK Button.



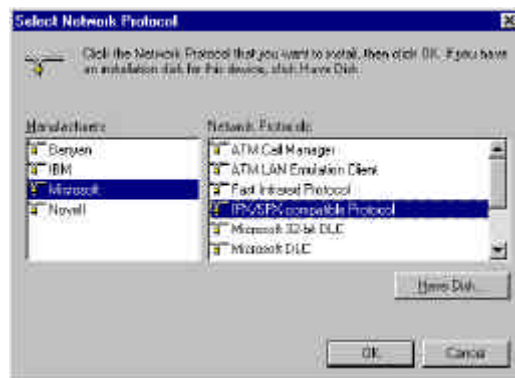
#### Add File & Print Sharing for MS Networks

1. Click the Add button
2. Select Services and click the Add button.
3. Choose Microsoft in the Manufacturers option box and File and Print Sharing for Microsoft Networks



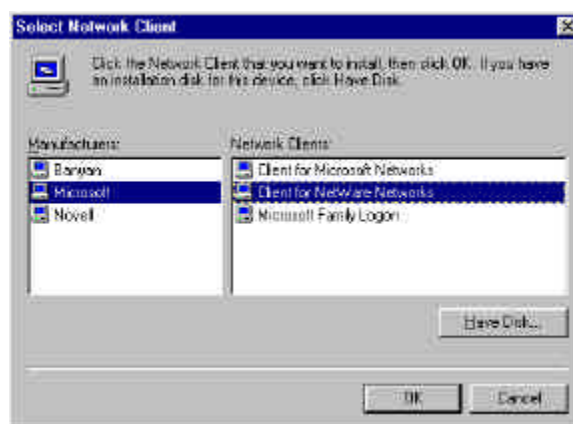
#### Add IPX/SPX Protocol

1. Click the Add button
2. Select Protocol and click the Add button.
3. Choose Microsoft in the Manufacturers option box and IPX/SPX Compatible Protocol in the Network Protocols option box.
4. Click the OK button.



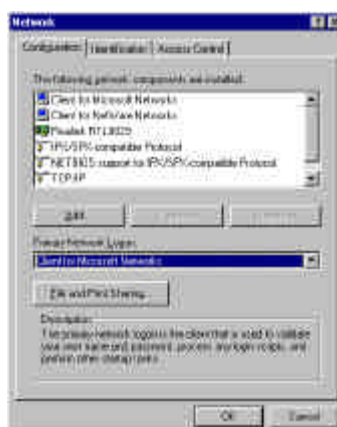
## Add Client for Netware Networks

1. Click the Add button
2. Select Network Client and click the Add button.
3. Choose Microsoft in the Manufacturers option box and Client for Netware Networks in the Network Clients option box.
4. Click the OK Button.



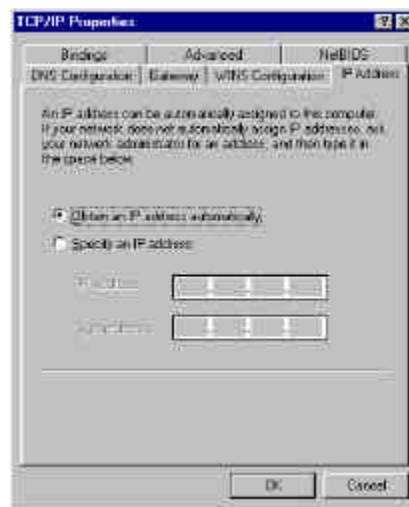
## Set your Primary Network Logon

In the Primary Network Logon drop down menu, select Client for Microsoft Networks.



## Setup Properties of Components

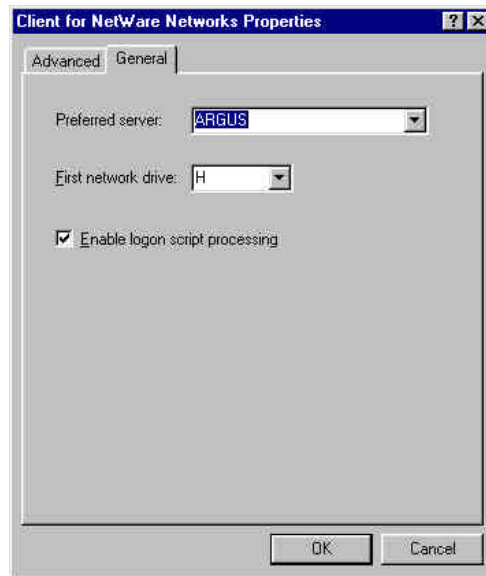
1. In 'The following components are installed' window, select TCP/IP -> Dial-up Adapter click the Properties button to open the TCP/IP Properties Screen. On the IP Address tab make sure Obtain an IP address automatically is selected and Press OK .



2. In 'The following components are installed' window, select and click the button. On the tab, enable the check box. In the Field enter the name of your Windows NT Domain and press .Client for Microsoft Networks Properties General 'Log On to Windows NT Domain' Windows NT Domain OK.



3. In 'The following components are installed' window, select Client for NetWare Networks and click the Properties button. On the General tab, in the 'preferred Server' enter the name of your Novell Netware Server Domain and select the First Network Drive and select Enable Logon Script Processing.



4. In 'The following components are installed' window, select IPX/SPX-compatible Protocol and click the Properties button. You must DISABLE Client for Microsoft Networks and File and printer sharing for Microsoft Networks. This will make sure that when you login to your NT your Windows 95/98 computer will use TCP/IP protocol. You also must ENABLE Client for Netware Networks.



## Set your Access Control

1. On the Network window select the Identification tab.
2. In the Workgroup field enter the name of your NT domain. If you are not sure What the name of your NT domain is, please ask the administrator of your NT server.
3. Enter a name for your computer and a description of your computer in the Computer name And Computer Description fields. These are for personal use only and can be anything you wish.



## Set your Identification

1. In the Network window select the Access Control tab.
2. In the 'Control Access to shared resources using:' option box, select Shared Level Access Control.



NOTE : Now you must restart your Windows 95/98 in order to have the setting that you made to take effect.

### Make your New Connection

1. Double Click the My Computer icon on your Desktop.
2. Open up your Dial-up Networking Folder.
3. Configure a new dial-up connection by double clicking the Add New Connection button.
4. Follow the instructions to completion.

### Set Dial-up Type

1. After you have made your new connection, select it, click the right mouse button and Select Properties.
2. Click the Server Type button and select PPP : Windows 95, Windows NT 3.5, Internet.
3. Enable ONLY Log on to Network, Enable Software Compression, IPX/SPX And TCP/IP As shown in the diagram.

### Dial-up your network device

You are ready to dial-up your network device. Double click on the new connection that you have made and enter the user name and password that is configured for you in your network device. Press the Connect button. After you have connected to your network device, your remote Windows 95/98 computer will behave exactly like a real node on your network.

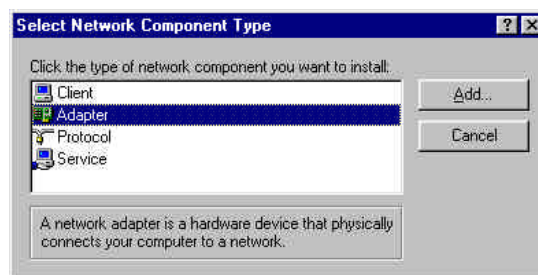
## Setting up a Remote Windows 95/98 Client to access a Unix Server

### Open Your Windows 95/98 Client Network Window

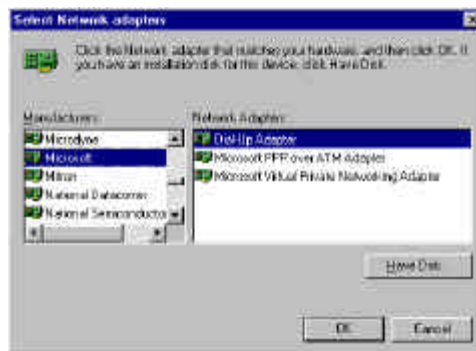
1. In the Windows 95/98 start menu, point to Settings and click Control Panel.
2. Double click the Network icon to open the Network Properties Display.

### Add Microsoft Dial-up Adapter:

1. Click the Add button
2. Select Adapter and click the add button.

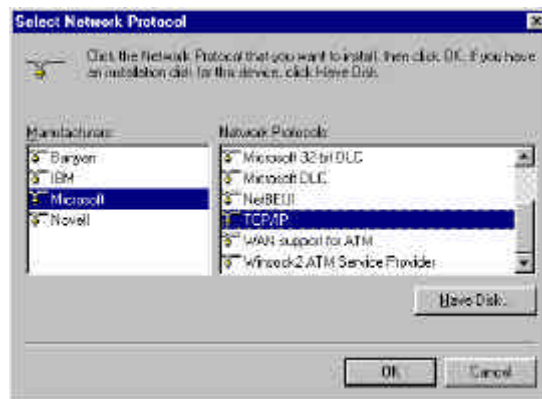


3. Choose Microsoft in the Manufacturers option box and Dial-up adapter in the Network adapters option box. Click the OK Button.



## Add TCP/IP Protocol

1. Click the Add button
2. Select Protocol and click the Add button.
3. Choose Microsoft in the Manufacturers option box and TCP/IP in the Network Protocols option box.
4. Click the OK Button.



## Setup Properties of Components

In 'The following components are installed' window select TCP/IP -> Dial-Up Adapter and click the Properties button to open the TCP/IP Properties Screen. On the IP Address tab make sure Obtain an IP address automatically is selected and press OK .



NOTE : Now you must restart your Windows 95/98 in order to have the settings that you made to take effect.

### Make Your New Connection

1. After you have made your new connection, select it, click the right mouse button and Select Properties.
2. Click the Server Type button and select PPP : Windows 95, Windows NT 3.5, Internet
3. Enable ONLY Enable Software Compression and TCP/IP as shown in the diagram.

### Set Dial-up Type

1. Double Click the My Computer icon on your Desktop.
2. Open up your Dial-up Networking Folder.
3. Configure a new dial-up connection by double clicking the Add New Connection button.
4. Follow the instructions to completion.

### Dial-up your network device

You are ready to dial-up your network device. Double click on the new connection that you have made and enter the user name and password that is configured for you in your network device. Press the Connect button. After you have connected to your network device, your remote Windows 95/98 computer will behave exactly like a real node on your network.

## LAN-to-LAN Settings

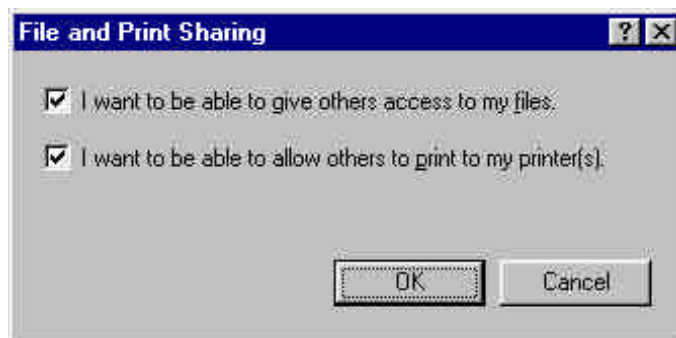
### Setting up LAN-to-LAN Routing

For LAN-to-LAN routing most of the settings was done in the Net-Device Utilities when you configure IP routing (NAT Disable) in your network device. This section will give you an overview on how to make LAN-to-LAN routing easier and show you some of the benefits and limitations of LAN-to-LAN routing.

### Setting up Windows 95/98 as a File Server

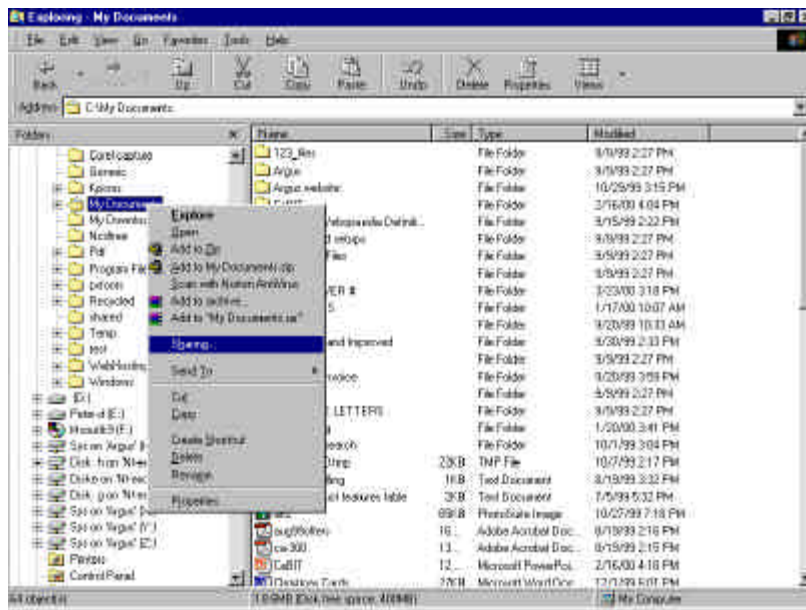
If you would like to share files over your network but don't want to have to install Windows NT you can also use Windows 95/98 to share files. To setup your computer for file sharing:

- A. On the Windows 95/98/NT/2000 **Start** menu, point to **Settings** and click **Control Panel**. Click the **Network** icon to open the Network window.
- B. Click the **File and Printer sharing** button
- C. Enable the **I want to be able to give others access to my files** selection.



- D. If you haven't already done so, you should make sure to give this computer a fixed IP address on your network. To do this, in the same Network window as figure 5-1 (page 5-1), select **TCP/IP** in the **The Following Network Components are Installed** window and click **Properties**. Here you can give this computer a unique IP address on your network. You will then have to reset your computer for the settings to take effect.

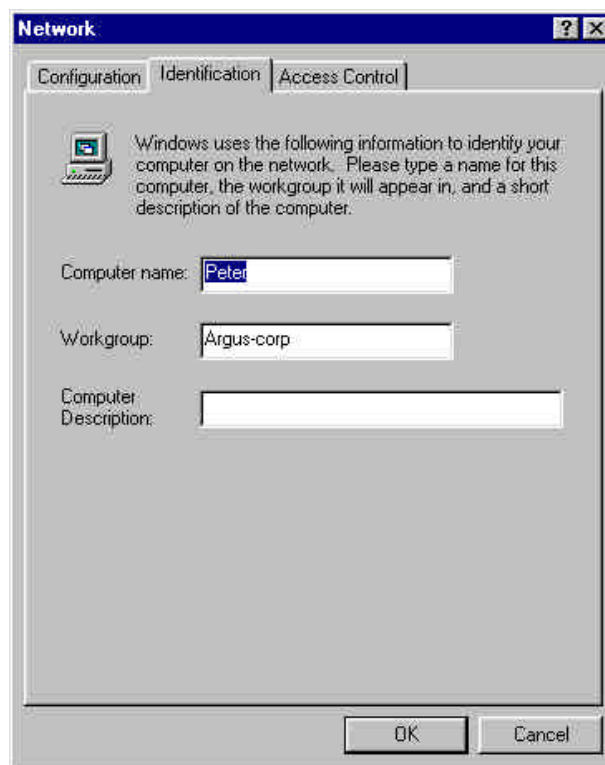
E. Use the **My Computer** directory structure to find the drive or file on this computer that you want to make available for sharing. Right Click on the file or drive that you want to share. Select **Sharing**.



F. Enable sharing by selecting **Shared As**. Choose the name that you want to give this computer on your network and the other options.



G. You also must make sure that computers that you want to use this sharing function are in the same workgroup. In the original network window select the Identification tab. If for example you set the Workgroup name for this computer as Argus-corp you should set the Workgroup name on the other computers that want to access this computer as Argus-corp.

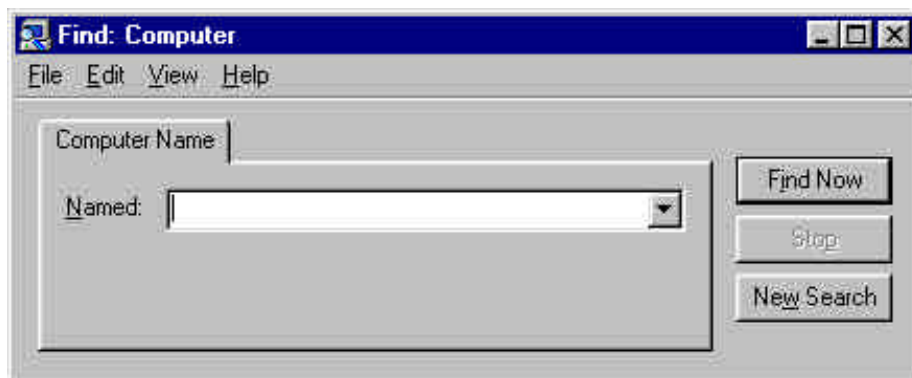


H. This computer can now be shared. You can use the **Find Computer** command on the next page to locate this computer's file across a network.

### Using the FIND COMPUTER Command

If your clients are in different subnets or are separated by a router, you will not be able to use the **Network Neighborhood** function in Windows 95/98/NT to see them.

What you can do however is use the **Find Computers** function of your Windows computer. Press the **Start** button and point to **Find** and then to **Computer**. A dialog box will be shown like below:



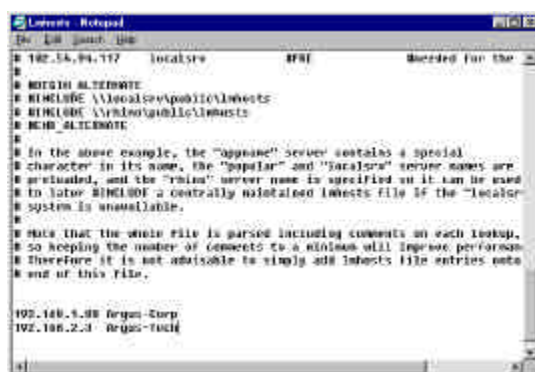
In the **Named** dialog box, type in the IP address of the computer you want to find. If you choose a computer that is on a remote network, it will cause your network device to dial-up a connection to the remote LAN based upon the settings that you inputted using the Net-Device Utilities.

**Note :** Please note that if the computer you are trying to access is on a remote LAN, you may have to press the **Find Now** button more than once to wait for your network device to dial-up a connection to your remote LAN.

## Using LMHOSTS

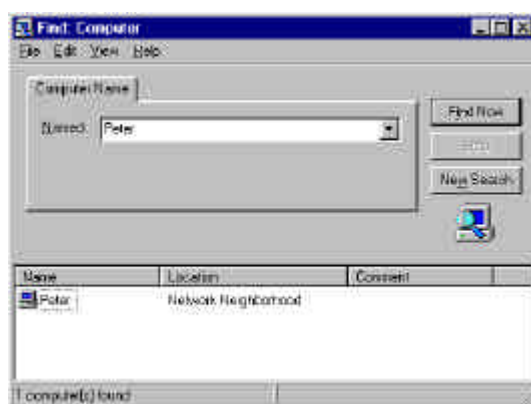
When using the **Find Computer** command, if you would rather enter the actual names of computers instead of the IP address, you need to enter them in a lookup table that is located in your Windows 95/98/NT computer called **lmhosts**. This file can be found in **C:\WINDOWS** file directory where **C** is the location of your Windows operating system.

This file can be edited in any text editor like **Notepad**. At the end of the file, you can enter the IP address plus a space and the computer name that is associated with this IP address. Please note the computers that you put in this lookup table should have fixed IP address on your LAN as they will be servers on your network. At the end of the file you should enter the IP address, a space and then the computer name with the IP address. In the example below we have entered into the lmhosts file and enter the computer named Argus-Corp has having an IP address of 192.168.1.88 and the computer named Argus-Tech has having an IP address of 192.168.2.3



After you have mapped the names of the computers to the IP address you should then copy this file over to the other computers on your LAN as each computer needs to have this lookup table to use this function.

After this is done, each computer on your LAN will be able to enter the name of the computer that they want to access on the LAN without having to remember the IP address. In our example below we have done a search for the computer called **Peter** and the search results is as shown below.



## Trouble Shooting

### Problem #1

**My computer can't detect my network device on the LAN when I start one of the Net-Device Utilities. (ie Device Not Found')**

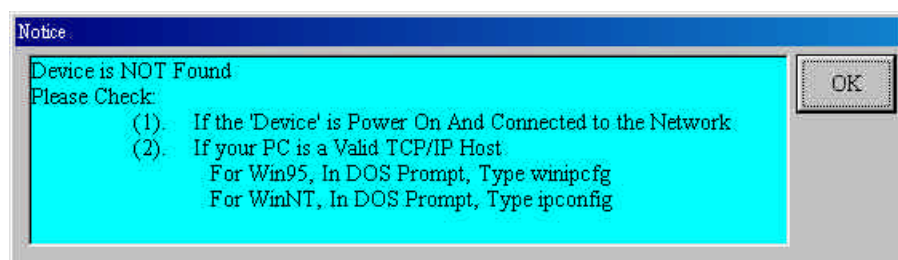
--Try pressing the **'Refresh Device List'** button.

- Unplug your network device and plug it back in and press the **'Refresh Device List'** Button.

- Make sure your computer is a properly configured TCP/IP computer. Check by trying to 'ping' the computer you are using. If you can successfully ping yourself, your computer has TCP/IP correctly installed. Then try pinging another computer on your network. If ping is successful, your computer is properly connected to the Network.

- Take TCP/IP Dial-up Adapter off your computer. For instructions on how to do this please see **Problem #2** on the next page.

- Make sure that your network device is properly connected to your Ethernet hub by Pressing **'Refresh Device List'** in either **Net-Device Manager** or **Setup Wizard**. If your network device is correctly connected, the 'Net' indicator light on your network device will flash. If no flash occurs, it is not properly connected to your network. Reconnect your network device to your hub and try again. If there is still no flash, it is possible our Ethernet cable or hub has a problem.



Device is NOT Found Screen

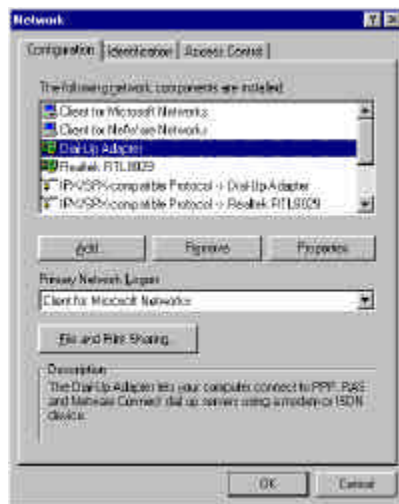
## Problem #2

**Other computers can connect to the network device but my computer can't.**

Whenever I click on Internet Explorer or Netscape I still see the Windows Dial-up Utility popping up on my screen asking for my phone number and password to dial-up my ISP.

- Take TCP/IP dial-up adapter off all computers that will be using your network device to access Internet. TCP/IP dial-up adapter is not needed to use your network device to connect to the Internet.

To take off TCP/IP **Dial-up Adapter** , on the Windows **Start** button, point to settings and then to **Control Panel**. Double click on the Network icon. Click on the adapter called **Dial-up Adapter** and press the **Remove** button. Restart your computer and try again.



Network Settings Screen

- Make sure that you have a correct IP address. On the Windows 95/98 Start button, select **Run** and type ``winipcfg`` . If the IP address field is listed as ``0.0.0.0`` that computer has no IP address. Make sure that the automatic DHCP configuration is setup properly on that computer.
- Make sure that the Web browser is set to connect via your LAN.

### Problem #3

I tried to upgrade the firmware on my network device and after the upgrade failed it is not listed in the Net-Device Utilities `Device List`.

- 1) On the side or back of your network device there is a switch marked **Terminal/Nomal**. Set the switch to **Terminal** which will manually put your network device in the configuration mode.
- 2) Unplug the power adapter of the device and plug it back.
- 3) After you have done this press the **Refresh Device List** in Net-Device Manager which should display your network device.
- 4) Go into the **Upgrade Firmware** menu and upgrade the firmware again until successful.
- 5) On the side or back of your network device set the switch back to Normal which will manually put your network device back into working mode.
- 6) Unplug the power adapter of the device and plug it back, and that`s it.

### Problem #4

The Network Device is connected to the Cable modem/ADSL, but has problems accessing the Internet.

- 1) Make sure your computer is configured properly as a TCP/IP workstation.
- 2) Try to ping the IP address of the Network Device (LAN Ethernet IP address)
- 3) Use **Network Monitor** to see if WAN Ethernet port has successfully acquired IP settings from ISP. Or if is it manually assigned a valid IP address from ISP.
- 4) Use **Winipcfg** to check if your computer`s IP settings are correct.

Please check if:

- a) DNS IP address is correct.
- b) Gateway IP address is the device`s LAN Ethernet IP address. (Server IP address)
- c) IP address/Network mask is correct.



IP Configuration Screen

#### **Problem #5**

**When I install the Net-Device Utilities I get the error message `missed export file Oleaut32.dll`**

- This is because your Win95/98/NT computer has an old version of the **oleaut32.dll** File.

- 1) Download the newest **oleaut32.dll** file.
- 2) Go into the directory C:\WINDOWS\SYSTEM\ and backup your old oleaut32.dll to a temporary directory.
- 3) Copy the new file you download to the directory C:\WINDOWS\SYSTEM.  
When Windows asks you if you want to replace the existing oleaut32.dll click yes.
- 4) After you have successfully copied the file over install the Net-Device Utilities.
- 5) If you have problems upgrading the file, you can use the backup copy to restore the original file.

#### **Problem #6**

**I configured my network device but I can't get it to communicate with my modem.**

- It's possible that your initial string is configured incorrectly. If you are using an ISDN TA and your ISDN TA was not listed, when you were prompted to select your modem in Setup Wizard you must look up your ISDN TA's initial string in your ISDN TA user's manual and input it in Net-Device Manager's Modem Settings Menu to correct this problem.

- If after making sure that the initial string is correct, your network device will still not dial-up a phone number, please use the Net-Device Monitor which has on-line help.

#### **Problem #7**

##### **My network device dials-up a connection but can't seem to communicate with the ISP.**

- This is most likely a problem due to the fact that your baudrate setting is set too high for your modem or ISDN TA. The maximum baudrate that your modem or ISDN TA claims it can achieve is often not really attainable because of poor phone line quality, modem manufacturing quality and a myriad of other possible reasons. You should go into Net-Device Manager's Modem Settings menu to correct this problem to set to a lower baudrate and try again.

- If after changing the baudrate, your network device still cannot connect to your ISP, please use the Net-Device Monitor which has on-line help.

#### **Problem #8**

##### **Sometimes when I try and use the Internet or get my mail, the application can't access the Internet immediately.**

- This is probably not an error or a problem. If you are the first person to use your network device, there will be a delay while the Dial-On-Demand function automatically dials-up a connection and logs on to your Internet Service Provider. Subsequent users will then be able to use the existing connection that you have just established without a delay.

- It is also possible that your modem is dialing but having problems connecting to your ISP. For Example your ISP may be returning a busy signal. You can use the Net-Device Monitor to see all events occurring between your modem and ISP.

#### Problem #9

##### **My network device seems to slow down my modem when I install it.**

- Your network device should have no effect on your modem speed. Of course if more than one client is using the same modem through your network device the speed will be reduced.
- Run **Network Monitor** Utilities to see how many clients are currently accessing the Internet.

#### Problem #10

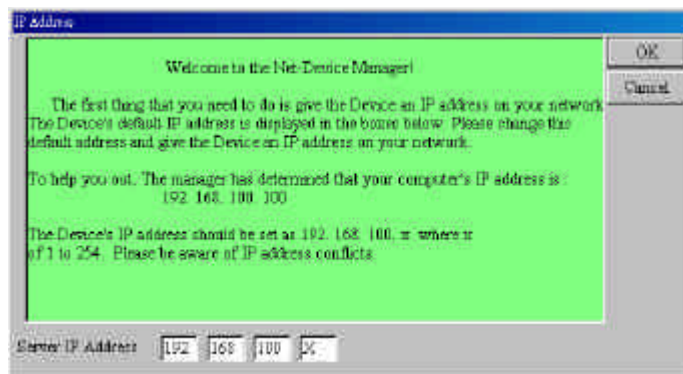
My Network Device keeps dialing-up a connection but nobody is using the Internet.  
(While Async port is in used)

- The Network Device will only dial-up a connection if there is a request from one of the computers on your LAN for an IP address on the Internet. There are some programs that are programmed to request information from the Internet. For example, Microsoft Outlook can be programmed to `Check for new mail every X minutes`. If you have this function enabled, Outlook will send out a request for your Internet POP3 server which will cause your Network Device to dial-up your ISP. To find out which computer on your LAN is the culprit, you can see the **Net-Device Monitor**'s event messages which will tell you which computer is causing the dial-up and also what service (port#) the computer is requesting.

### Problem #11

The 'Please set the device IP' screen displayed when configuring the Device.

The screen displays when the manager has detected the device's IP address (LAN Ethernet IP address) is not in the same subnet as the PC's. You will have to set the device's IP address to the same network as your PC's and click **OK**. The manager will set the device's IP address.



IP Address Screen

### Problem #12

The server's IP address conflicts with another server in the network screen displayed when running Net-Device Manager.

- The manager has detected the IP address of the Network Device you are configuring is conflicting with another device. You should power off the conflicting device and configure Network Device with a different LAN (Server) IP address.



IP Conflict screen

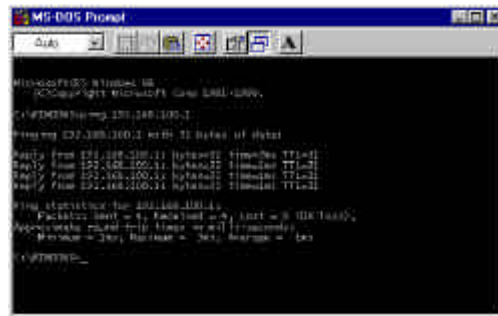
## Tools for your Net Device

### Net-Device Monitor

So you're having some problems. Many problems can be solved by checking out the Net-Device Monitor where there is on-line help. Please see Section - 4 **Net-Device Monitor** which details all its functions and help applications.

### PING

Ping stands for Packet Internet Groper. Ping is a utility that conducts a test to determine if there is a communications path between two devices on a network. Basically it lets your computer ask another computer or device, 'is there anything alive at this IP address?'. You can use the PING command in your DOS prompt. You can also type the IP address to the domain name of the Net-Device you wish to PING. For example both 'PING 213.0.0.2' and 'PING www.abc.com' will work. In the example below we have sent a successful PING to an Network Device which has an IP address of 192.168.100.1. Your computer will see if there is a connection between your computer and your Network Device. You can also ping an IP address on the Internet to make sure that your computer has a connection via the RAS to the Internet. It's a great way to eliminate some of the potential reasons for troubles.

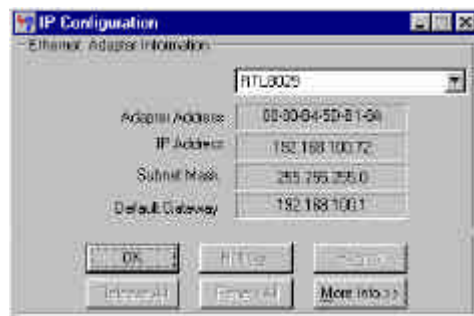


### WINIPCFG and IPCONFIG

There two tools which are great for finding out a computer's IP configuration, MAC address and default gateway.

1) WINIPCFG (for Windows 95/98) :

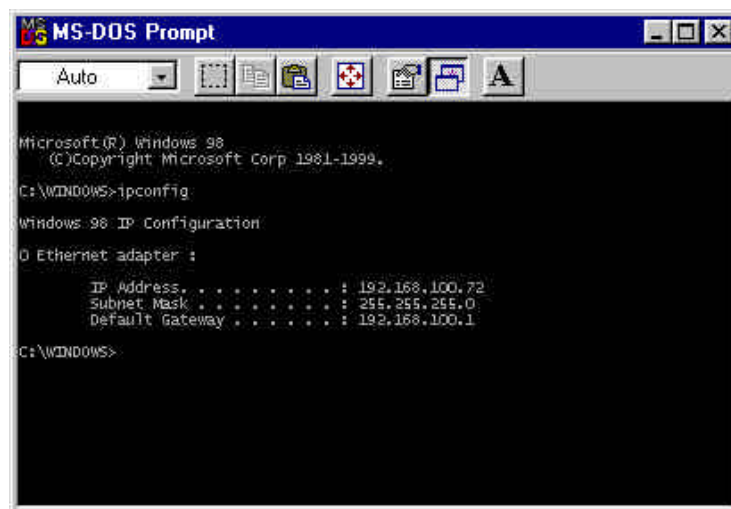
On the Windows 95/98 **Start** button, select **Run** and type **wipnfcfg**. In the example below this computer has an IP address of 192.168.100.72 and the Default Gateway Is 192.168.100.1. The default gateway should be the Network Device IP address. The MAC address in Windows 95/98 is called the Adapter address.



## 2) IPCONFIG (for Windows NT) :

In the DOS command type **IPCONFIG** and press **enter**.

Your computer's IP information will be displayed as shown below.



```
MS-DOS Prompt
Auto
Microsoft(R) Windows 98
(C)Copyright Microsoft Corp. 1981-1999.
C:\WINDOWS>ipconfig

Windows 98 IP Configuration

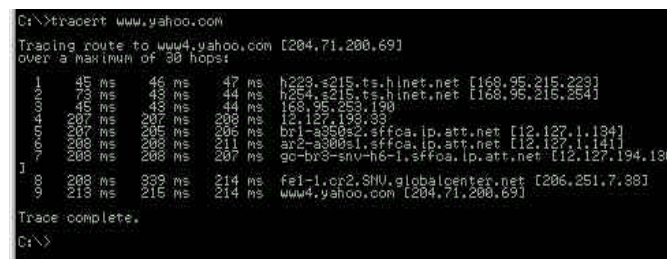
Ethernet adapter :

    IP Address. . . . . : 192.168.100.72
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.100.1

C:\WINDOWS>
```

## TRACERT

Tracert is an extension of the PING utility that lets you trace the route to an IP address. It reports the number of router hops, the time for each hop, and any failed attempts to cross a hop. In this way you can locate the specific site of a failed Ping. You can run Tracert in the DOS prompt. In the example below we have traced a request for [www.yahoo.com](http://www.yahoo.com) by typing in Tracert `C:\>Tracert [Www.yahoo.com](http://www.yahoo.com)`



```
C:\>tracert www.yahoo.com
Tracing route to www4.yahoo.com [204.71.200.69]
over a maximum of 30 hops:
  0  45 ms  46 ms  47 ms  h223-215.ts.hinet.net [168.95.215.223]
  1  73 ms  44 ms  44 ms  h223-215.ts.hinet.net [168.95.215.223]
  2  45 ms  40 ms  44 ms  168.95.253.190
  3  207 ms  208 ms  208 ms  12.127.194.138
  4  207 ms  208 ms  208 ms  br1-as3082.sffca.ip.att.net [12.127.1.134]
  5  208 ms  208 ms  211 ms  sr2-as3081.sffca.ip.att.net [12.127.1.141]
  6  208 ms  208 ms  207 ms  gc-br3-snv-h6-1.sffca.ip.att.net [12.127.194.138]
  7  208 ms  208 ms  214 ms  fe1-1.cr2.SNU.globalcenter.net [206.251.7.88]
  8  219 ms  216 ms  214 ms  www4.yahoo.com [204.71.200.69]

Trace complete.
C:\>
```

## Glossary

**Baudrate** Baudrate in regards to your network device refers to the number of bits per second (Bps) that are transmitted between your network device and modem or ISDN TA.

### DHCP (Dynamic Host Configuration Protocol)

A protocol that was made to lessen the administrative burden of having to manually configure TCP/IP Hosts on a network. DHCP makes it possible for every computer on a network to extract its IP information from a "DHCP server" instead of it having to be inputted manually by each network client (or network administrator). Using the DHCP server built-in to your network device, every computer on your network can automatically extract its IP information from your network device.

#### Why is it called "dynamic"

Each time a network client turns on their computer your network device DHCP server will automatically give them an IP address from the IP address pool configured in the DHCP Server menu of Net-Device Manager. It is called "dynamic" because the address that they get could be different each time they turn on their computer depending on which addresses have already been assigned.

**DNS (Domain Name System)** Server IP Address. A DNS Server can be thought of as the computer at your ISP whose job is to take all the DNS addresses that you type into your web browser like [www.yahoo.com](http://www.yahoo.com) and translate those addresses into their corresponding IP addresses. So to send this "translator" all your requests for information, you need to know his address and his address is known as the DNS Server IP address.

**Ethernet** A LAN (Local Area Network) protocol developed by Xerox and DEC. It is a very commonly used type of LAN

**Firewalls.** A method of protecting files and programs on one network from users on another network. Firewalls are typically installed to give users access to the Internet while protecting their Internal Information. Your network device uses a firewall known as NAT. (See NAT).

**Firmware.** Software that has been permanently or semi-permanently written onto ROM. Your network device supports flash ROM which means you can upgrade the firmware in your network device very easily by obtaining a copy of the new firmware and using the upgrade firmware function.

**FTP (File Transfer Protocol).** A protocol which allows a user on one host to access, and transfer files to and from, another host over a network.

**Intranet.** The Intranet is the use of Internet technologies within a company. Intranets exist only within organizations while the Internet is a global network open to all. Intranets run on private networks within companies and between their branch offices.

**IP (Internet Protocol).** The Internet Protocol is the network layer for the TCP/IP Protocol Suite. It is a connectionless, best-effort packet switching protocol.

### **IP Addresses**

A Computer on the Internet is identified by its **IP Address**. A computer's IP address is like a telephone number because it identifies one address or in this case one computer Device. Every computer or device on a network must have a different IP address. An IP address consists of four groups of numbers called **octets** which are separated by periods. For example, 213 . 0 . 0 . 1 is an IP address. An IP address consists of a **network portion** and a **host portion**. The network portion identifies the subnet that the computer belongs to. The host portion identifies the particular computer or node on that network. In our example IP address, **213 . 0 . 0 . 1** refers to the network **213 . 0 . 0** with the host number **1**. IP addresses can either be dynamic (temporary) or static (permanent, fixed). A dynamic IP address is a temporary IP address that is assigned to you by a server (Usually a DHCP server) when you turn on your computer. A static IP address is a permanent IP address that you can set yourself in your computer. When your network device dials-up your ISP your ISP can give it a fixed or dynamic IP address. Likewise when you turn on your computer your network device can give your computer a dynamic or fixed IP address.

**ISDN TA.** (Integrated Services Digital Network Terminal Adapter) ISDN is a high speed digital telephone connection involving the digitization of the telephone network using existing wiring. An ISDN Terminal Adapter can be thought of as an “ISDNModem”.

**ISP (Internet Service Provider).** An organization that provides Internet services. An ISP is the company that will provide the connection from your computer or network to the Internet. An ISP can offer a range of services, such as dial-up accounts, E-mail, web hosting or News.

**LAN (Local Area Network).** A data network intended to serve an area of only a few square kilometers or less. This often means a small private network in companies.

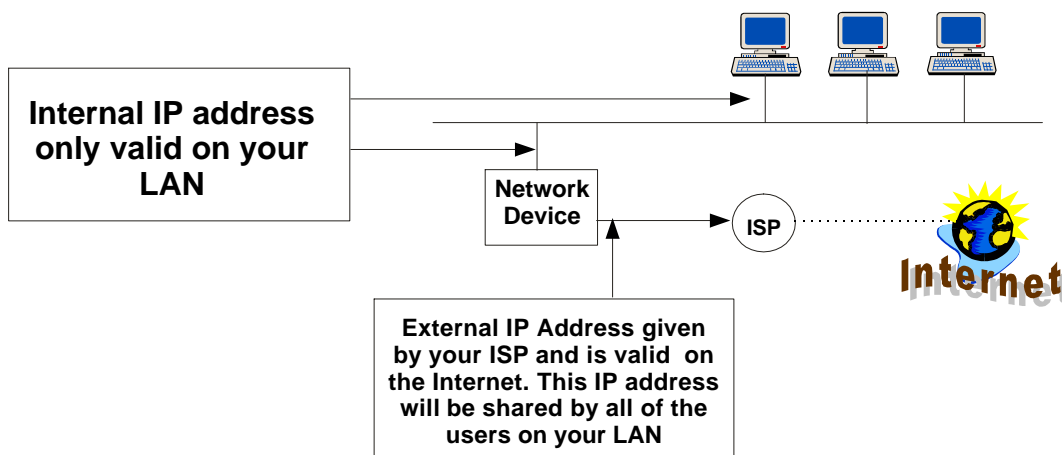
**ML-PPP (Also called MP or MPPP)** stands for Multilink Point to Point Protocol and is an advancement of the PPP protocol that allows for the bridging or bundling of two ISDN or analog channels for faster connections. What does that mean in practical terms? It means that you can use one computer to use two or more modems to download a single web page. For example, if I'm trying to access [www.yahoo.com](http://www.yahoo.com) using two modems, each modem will go get part of Yahoo, then your network device will bundle the information together and then give it to your computer resulting in double the speed.

**MAC address.** The hardware address of a Device connected to a shared media. To find out the MAC address of your computer please see [Troubleshooting](#).

## NAT Technology

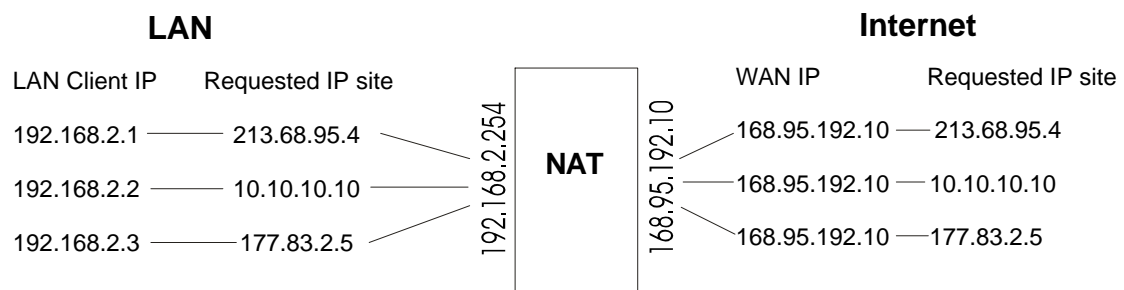
Your network device uses a technology called Network Address Translation (NAT) (Sometimes called IP Address Masquerading) to let everyone on your network use one IP address given to you by your ISP (Internet Service Provider). This technology is also a firewall in itself.

How does it work? Every IP address on the Internet is a Registered or Legal IP address. Therefore no two IP addresses on the Internet are the same. For you to use your network device to access the Internet you need one of these registered IP address from your ISP (Internet Service Provider). On your private Intranet or LAN, the IP addresses of your computers are probably unregistered or “illegal” IP addresses.



When clients on your network start surfing the Internet, your network device will receive all the requests for information. Your network device will dial-up your ISP and your ISP will give your network device a registered legal IP address. Your network device then uses that IP address to request information saying, “Send all information back to me at this IP address.” So in essence it looks like all your network clients’ requests are coming from that one IP address (Hence the name IP masquerading). When all that information comes back to your network device, it will then sort the data out using an Address Translation Table and give the data to the computer on your network that requested it.

In regards to the firewall, what happens if someone on the Internet tries to access your network via your network device? Nothing! There's nothing there but your network device which will not reverse translate unless you have allowed it by using the Virtual Server function (IPMapping).



**Network Address** The network portion of an IP address. For a class A network, the network address is the first byte of the IP address. For a class B network, the network address is the first two bytes of the IP address. For a class C network, the network address is the first three bytes of the IP address. In each case, the remainder is the host address. In the Internet, assigned network addresses are globally unique.

**Port Number.** In addition to meaning a connector on your computer, a port also has another meaning. The other meaning of port can be thought of as a "Service number". Every service that travels over phone lines and modems has a standard port number. For example to use the World Wide Web service the standard port number is **80**. The standard port number for telnet is **23**. Who came up with this system? Port numbers are controlled and assigned by the IANA (Internet Assigned Numbers Authority). How do you know what service has what port number? Most computers have a table in their systems that lists which port numbers have been assigned to which services or you could also find port number lists on the Web.

**Protocol.** A formal description of message formats and the rules two computers must follow to exchange those messages. You can think of protocols like languages. If two computers or devices aren't speaking the same language to each other, they won't be able to understand or communicate. Just like people!

**PPP (Point-to-Point Protocol).** PPP enables dial-up connections to the Internet and is the method that your network device connects to the Internet. PPP is more stable than the older SLIP protocol and provides error checking features.

**Router.** A device which forwards traffic between networks. If you request information from a location on your network or the Internet the router will route the request to the appropriate destination. The router's job is to listen for requests for IP addresses that are not part of your LAN and then route them to the appropriate network which may either be the Internet or another subnetwork on your LAN.

**Server.** A provider of resources (e.g., file servers and name servers). A computer that uses the resources of a server is called a **Client**. For example your network device provides Internet Access and is thus called an Internet Access **Server**.

**Subnet:** A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP Addresses have the same prefix. For example, all devices with IP addresses that start with 213 . 0 . 0 . would be part of the same subnet.

**Subnet Mask / IP Address Mask.** Subnet mask is what is used to determine what subnet an IP address belongs to. Subnetting enables the network administrator to further divide the host part of the address into two or more subnets.

**TCP/IP (Transmission Control Protocol/ Internet Protocol )** is the standard protocol used on the Internet. This means that every computer that wants to communicate with another computer on the Internet must use TCP/IP protocol to transmit and route data packets. TCP/IP uses **IP addresses** to locate different computers or devices on a network.

**UDP (User Datagram Protocol).** An Internet Standard transport layer protocol. It is a connectionless protocol which adds a level of reliability and multiplexing to IP.